ENSURING THE SECURITY OF AMERICA'S BORDERS THROUGH THE USE OF BIOMETRIC PASSPORTS AND OTHER IDENTITY DOCUMENTS

HEARING

BEFORE THE

SUBCOMMITTEE ON ECONOMIC SECURITY, INFRASTRUCTURE PROTECTION, AND CYBERSECURITY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

JUNE 22, 2005

Serial No. 109–24

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE
26–515 PDF WASHINGTON : 2005

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

CHRISTOPHER COX, California, *Chairman*

DON YOUNG, Alaska
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
CHRISTOPHER SHAYS, Connecticut
PETER T. KING, New York
JOHN LINDER, Georgia
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
JIM GIBBONS, Nevada
ROB SIMMONS, Connecticut
MIKE ROGERS, Alabama
STEVAN PEARCE, New Mexico
KATHERINE HARRIS, Florida
BOBBY JINDAL, Louisiana
DAVE G. REICHERT, Washington
MICHAEL MCCAUL, Texas
CHARLIE DENT, Pennsylvania
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida

SUBCOMMITTEE ON ECONOMIC SECURITY, INFRASTRUCTURE PROTECTION, AND CYBERSECURITY

DANIEL E. LUNGREN, California, *Chairman*

DON YOUNG, Alaska
LAMAR S. SMITH, Texas
JOHN LINDER, Georgia
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
MIKE ROGERS, Alabama
STEVAN PEARCE, New Mexico
KATHERINE HARRIS, Florida
BOBBY JINDAL, Louisiana
CHRISTOPHER COX, California *(Ex Officio)*
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
PETER A. DEFAZIO, Oregon
ZOE LOFGREN, California
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
JAMES R. LANGEVIN, Rhode Island
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

CONTENTS

ENSURING THE SECURITY OF AMERICA'S BORDERS THROUGH THE USE OF BIOMETRIC PASSPORTS AND OTHER INDENTITY DOCUMENTS

Wednesday, June 22, 2005

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON ECONOMIC SECURITY,
INFRASTRUCTURE PROTECTION, AND CYBERSECURITY
COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The subcommittee met, pursuant to call, at 11:04 a.m., in Room 2257, Rayburn House Office Building, Hon. Dan Lungren [chairman of the subcommittee] presiding.

Present: Representatives Lungren, Cox, Linder, Souder, Pearce, Sanchez, Thompson, Dicks, Christensen, Lofgren, and Langevin.

Mr. LUNGREN. [Presiding.] The Committee on Homeland Security, Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity will come to order.

The subcommittee is meeting today to hear testimony on ensuring the security of America's borders through the use of biometric passports and other identity documents.

I would like to start by thanking the witnesses on both panels for being with us today and on relatively short notice.

The purpose of today's hearing is to examine the current and future use of biometric technology in travel documents. The issues of document integrity and identity verification are key to our national efforts to enhance border security and combat terrorist travel.

Today's hearing provides an opportunity to examine progress made in this area by reviewing two recent announcements by the Department of Homeland Security: Number one, the changes in the passport requirements for Visa Waiver Program travelers and, two, the pilot program to test the use of contact with chips in passports.

On June 15, 2005, the Department of Homeland Security announced that Visa Waiver Program countries would be required to producer tamper-resistance digital photographs on newly issued passports, beginning on October 26, 2005. Within another year their passports would be required to have an integrated chip capable of storing biographic and biometric information.

The announcement grew out of requirements enacted into law as part of the Enhanced Border Security and Visa Entry Reform Act of 2002, which required that each visa waiver country government certify by October 26, 2004 that it had established a program to issue tamper-resistance, machine-readable passports that incor-

porate a biometric identifier matching standards established by the International Civil Aviation Organization.

Faced with the certainty that very few countries would meet the original deadline, last year Congress approved an extension of the deadline by an additional year to October of 2005. The announcement last week represents the Department's proposed compromise between the administration, the Congress and the VWP countries, many of whom would have still failed to meet the deadline had the Department of Homeland Security insisted that the Visa Waiver Program country passports actually contain a biometric chip as of the date, October 2005.

I look forward to hearing from our witnesses about the rationale behind these decisions, how these new requirements will strengthen security and actually be implemented in the field and how they will be integrated with existing security programs, particularly US–VISIT.

I also look forward to exploring the security limits of our strategy, as outlined to date, particularly with respect to the use of biometrics to actually help us confirm traveler identity and screen for potential terrorists, criminals and immigration law violators.

With over 15 million Visa Waiver Program travelers entering the United States each year, travel facilitation is essential, as is ensuring that this program will not become an avenue for terrorists to gain entry into the U.S.

The 9/11 Commission report released last year highlighted the issue of terrorist travel and terrorist exploitation of travel documents. The Commission report stated, in part, "Terrorists must travel clandestinely to meet, train, plan, case target and gain access to attack." In their travels, terrorists use evasive methods, such as altered and counterfeit passports and visas, specific travel methods and routes, liaisons with corrupt government officials, human smuggling networks, supportive travel agencies and immigration identity fraud.

Strengthening document security and our ability to verify travelers' identity is essential if we are to prevent terrorists easy access to America. Information sharing between governments is thus a critical layer in our security system. The Department's announcement last week also contained new requirements for the Visa Waiver Program countries concerning lost and stolen passports, and that is extremely important.

Having access to a list of potentially compromised passports will enable inspectors and consular officers overseas to have a greater ability to judge legitimate documents.

Finally, this hearing will provide the subcommittee with an opportunity to examine where the field of biometrics is headed and how with proper privacy safeguards this technology can be used to strengthen our capabilities to intercept, disrupt and prevent terrorists from entering the U.S.

Again, I thank the witnesses for being here and for the effort that went into their testimony.

Again, I thank our witnesses for being here, and for the effort that went into their testimony.

I now recognize the ranking member, the gentlelady from California, for any opening statement she may wish to make at this time.

PREPARED OPENING STATEMENT OF THE HON. DANIEL E. LUNGREN

I would like to start by thanking the witnesses on both panels for being with us today, and on relatively short notice. The purpose of today's hearing is to examine the current and future use of biometric technology in travel documents. The issues of document integrity and identity verification are key to our national efforts to enhance border security and combat terrorist travel.

Today's hearing provides an opportunity to examine progress made in this area by reviewing two recent announcements by the Department of Homeland Security (DHS):

1. changes in the passport requirements for Visa Waiver Program (VWP) travelers, and
2. a pilot program to test the use of contactless chips in passports.

On June 15, 2005, the Department of Homeland Security announced that Visa Waiver Program countries would be required to produce tamper-resistant digital photographs on newly-issued passports starting on October 26, 2005. Within another year, their passports would be required to have a integrated chip capable of storing biographic and biometric information.

This announcement grew out of requirements enacted into law as part of the Enhanced Border Security and Visa Entry Reform Act of 2002, which required that each Visa Waiver Country government certify by October 26, 2004, that it had established a program to issue tamper-resistant, machine-readable passports that incorporate a biometric identifier matching standards established by the International Civil Aviation Organization (ICAO). Faced with the certainty that very few countries would meet that original deadline, last year Congress approved an extension of the deadline by one additional year, to October of 2005.

The announcement last week represents the Department's proposed compromise between the Administration, Congress, and the VWP countries, many of whom would have still failed to meet the deadline had DHS insisted that the VWP country passports actually contain a biometric chip as of October 2005.

I look forward to hearing from our witnesses about the rationale behind these decisions, how these new requirements will strengthen security and actually be implemented in the field, and how they will be integrated with existing security programs, such as US–VISIT. I also look forward to exploring the security limits of our strategy as outlined to date, particularly with respect to the use of biometrics to actually help us confirm traveler identity and screen for potential terrorists, criminals, and immigration law violators.

With over 15 million VWP travelers entering the United States each year, travel facilitation is essential—as is ensuring this program is not an avenue for terrorists to gain entry to the U.S. The 9/11 Commission report, released last year, highlighted the issue of terrorist travel and terrorist exploitation of travel documents. The Commission report stated: "Terrorists must travel clandestinely to meet, train, plan, case targets, and gain access to attack. . .In their travels, terrorists use evasive methods, such as altered and counterfeit passports and visas, specific travel methods and routes, liaisons with corrupt government officials, human smuggling networks, supportive travel agencies, and immigration and identity fraud."

Strengthening document security and our ability to verify travelers' identity is essential to preventing terrorists easy access to America. Information sharing between governments is thus a crucial layer in our security system. The Department's announcement last week also contained new requirements for VWP countries concerning lost and stolen passports. Having access to a list of potentially compromised passports will enable inspectors and consular officers overseas to have greater ability to judge legitimate documents.

Finally, this hearing will provide the Subcommittee with an opportunity to examine where the field of biometrics is headed and how, with proper privacy safeguards, this technology can be used to strengthen our capabilities to intercept, disrupt, and prevent terrorists from entering the United States.

Mr. LUNGREN. I now recognize the Ranking Member, the gentlelady from California, for any opening she may wish to make.

Ms. SANCHEZ. Thank you, Mr. Chairman. First of all, let me thank you for holding this hearing. I think it is a very important hearing.

And thank the witnesses for presenting for us today.

I am pleased that we are holding this on biometric passports and other identity documents. I think these are two very specific passport initiatives. There are two very specific passport initiatives that I hope that our witnesses will address today. The first is the elimination of the Western Hemisphere passport exemption in the 9/11 bill, and the second is the Visa Waiver Program.

I represent a district in California. It is based on a lot of tourism. We have Disneyland, we have Los Angeles Airport not too far from us, the port is the third largest entry port of cargo coming in. We have a border to the south of us, about an hour and a half drive from where we are. And if there is a threat to our country, California would be one of the first places that we would look at and some of the other border states. So this is a very important issue to us about how people get in to our country.

I think we need to do everything we can to secure borders, but we have also got to understand that there is a lot of commerce that happens through the port, through the airport and across our land borders, and there is a lot of movement of goods and people. And it is critical for our economy, for our prosperity that we sort of get a handle on how we are moving things and how we are checking things come in.

So I am interested in hearing what the Department of Homeland Security and the State Department are doing to ensure that the implementation of the Western Hemisphere travel initiative goes smoothly.

And I would specifically to have you talk a little bit about what is happening or what you intend to happen at the security entry of travelers. We have SENTRI, we have NEXUS, we have FAST, which are all pre-enrollment programs, basically allowing expedited inspection in return for more information from the traveler.

Now we have the passport initiative, and now I hear that the Department of Homeland Security may allow the TSA's registered traveler card to be used as an alternate document to the passport.

So I want to know what impact all of these new initiatives, if any, will have on NEXIS, on SENTRI, on FAST. I have a lot of people in my area who have gone through extensive background checks, paid their money. I even know of some who have been denied because we have been looking at all of this. How is that going to affect the people who are already doing some of this?

And, finally, with regards to the Visa Waiver Program, I think that the biometric passports are important and they are part of the solution, but I do not know that they are entirely the solution. I mean, first of all, what control do we have over an issuing country's vetting process for how it makes its passport decisions, for example? And perhaps an even greater concern is the fact that the Visa Waiver Program traveler can still get on a plane to the United States without first being checked against our watch list.

So I think there are a lot of things here we need to get the details on, and there are some things we need to fix, Mr. Chairman, and I am looking forward to the testimony of our experts.

Mr. LUNGREN. I thank the gentlelady.

The Chair would now recognize the chairman of the full committee, the gentleman from California, Mr. Cox, for his statement.

Mr. COX. Thank you very much, Mr. Chairman. This is a very important hearing. I regret that we are in such a small room, because there is a long line of people outside who also want to be in here to observe these proceedings. So that is a testament, I think, to the importance of the topic that you put before the committee today.

The impetus for today's hearing, of course, is the recent policy announcement by DHS, as you described, Mr. Chairman, regarding implementation of the biometric passports requirements in the Visa Waiver Program. But I hope that this hearing will quickly move us beyond this specific decision to a broader discussion of how our nation can, working with other countries around the world, develop a system that is fast, reliable and affordable, and protective of personal privacy that will instantly establish a genuine biometric link between individuals and documents in order to confirm traveler identity.

At the same time, while we are making admirable progress in developing tamperproof IDs, we have got to focus renewed and redoubled attention on keeping official travel documents that are nicely tamperproof out of the hands of terrorists and other criminals. In this vein, we will discuss today the choice of facial recognition by the Department of Homeland Security in the form of a digitized photograph as the qualifying biometric for visa waiver country passports to meet the statutorily imposed deadline of October 26 of this year.

I want first to begin by commending the Department of Homeland Security and the Department of State for exercising flexibility and good judgment and not insisting on a biometrically encoded chip for visa waiver country passports by this October, since doing so would have caused severe disruption to legitimate trade and travel with little security benefit in return.

Now, I want to emphasize the importance of that connection. I think disrupting commercial activity if there is some security payback is at least worth discussing. But disrupting commercial activity without any appreciable security payback is not a wise decision.

The digitized photograph requirement will, in the short term, provide some additional security benefits in terms of tamper resistance. But even when we move to encoding the digital photographs into the passport chip, as ultimately called for under the Department's policy and the biometric standards established by ICAO, we will still be relying on a Customs and Border Protection officer to perform a visual comparison of the person's digital photograph against the actual person presenting himself or herself at the port of entry.

In other words, the use of digital photos on these visa waiver passports will only undergo a manual human verification of the passport holder's identity. It will not undergo a computerized check or any digital or authentically biometric check against either a database of photographs or a single photograph of the passport holder that was taken at the time of entry.

So the biometric requirement under current law is, in essence, a tool to help reduce tampering and fraudulent alteration of passports. That in itself is of course useful. But as currently designed, this biometric encoding of passports simply will not help us to con-

firm travelers' identities through the use of technology, such as matching digitized photographs or, better yet, fingerprints stored in travel documents and national and international databases against those of the traveler seeking entry at our ports.

We also need to focus on how terrorists can circumvent this biometric passport system through the use of false breeder documents, through the acquisition of lost and stolen passports or other ways and how we can make better use of all available information from our databases about known or suspected terrorists.

In short, we need to clarify what the goal is that we are trying to achieve. Are we merely trying to verify that the person to whom the official travel document was issued is the same person who is using the document to gain entry into the United States or are we seeking to deploy a comprehensive border security system, which begins at the time the travel document is created and issued?

I believe we should be moving toward an international system based on biometrics that screens people before they obtain travel documents so that we verify people are who they say they are and ensure that they are not suspected terrorists or criminals. The object, after all, is not to give terrorists or criminals tamperproof fake IDs.

I am pleased to hear that the Department of Homeland Security recognizes that this biometric requirement for visa waiver country passports is a starting point and not the ending point of this important discussion on how to combat terrorist travel. Both these passports and our own U.S. passports will be equipped with computerized chips that are able to accommodate additional biometric identifiers such as fingerprints.

I look forward to hearing from the Department of Homeland Security about its vision of border security through the use of biometric technology and how these passport requirements can ultimately be integrated with other programs aiming to achieve the same goal of ensuring secure and efficient travel, both within and across the U.S. borders, programs such as NEXIS, FAST, SENTRI, TWIC and Registered Traveler.

I am also pleased the Department does not intend to change its policy that visa waiver travelers must enroll in US–VISIT when they arrive at U.S. ports of entry. This program affords us the opportunity to check travelers' fingerprints against available databases to help determine if the person has a terrorist connection or otherwise has violated U.S. criminal or immigration laws. If visa waiver passports were encoded with fingerprints, we would also be able to match with much greater precision the identity of the passport holder to the person to whom the travel document was originally issued. I hope we can explore this and other issues during today's hearing.

I want again to thank our witnesses, I want to thank the chairman for scheduling this important hearing and the Ranking Member, and I of course yield back the balance of my time.

PREPARED STATEMENT OF THE HON. CHRISTOPHER COX

Thank you, Chairman Lungren for holding this hearing today on the very important issue of combating terrorist travel through the use of biometrics. And I, too, would like to welcome and thank all of our witnesses for their testimony today.

The impetus for today's hearing is, as Chairman Lungren described, the recent policy announcement by the Department of Homeland Security (DHS) regarding implementation of the biometric passport requirement for countries in the Visa Waiver Program—or VWP. But I hope that this hearing will quickly move us beyond this specific decision to a broader discussion of how our Nation can, working with other countries around the world, develop a truly secure system for confirming traveler identity and keeping official travel documents out of the hands of terrorists and other criminals.

In this vein, we will discuss today the choice of DHS to use facial recognition, in the form of a digitized photograph, as the qualifying biometric identifier for VWP country passports to meet the statutorily imposed deadline of October 26, 2005. I want to first begin by commending the Department of Homeland Security and the Department of State for exercising flexibility and good judgment in not insisting on a biometrically-encoded chip for VWP country passports by this October, since doing so would have caused severe disruption to legitimate trade and travel—with little security benefit in return.

The digitized photograph requirement will, in the short term, provide some additional security benefit in terms of tamper resistancy. But even when we move to encoding the digital photograph into the passport chip—as ultimately called for under the Department's policy and the biometric standard established by ICAO—we will still be relying on a CBP officer to perform a visual comparison of the person's digital photograph against the actual person presenting themselves at the port of entry. In other words, the use of digital photos VWP passports will only undergo a manual human verification of the passport holder's identity, but will not undergo a computerized check against either a data base of photographs or a single photograph of the passport holder taken at the time of entry.

The biometric requirement under current law is, in essence, a tool to help reduce tampering and fraudulent alteration of passports. That is, in itself, important and useful. But as currently designed, this biometric encoding of passports will not help us confirm traveler's identities through the use of technology—such as matching digitized photographs or, better yet, fingerprints stored in travel documents and national and international databases against those of the traveler seeking entry at our port.

We also need to focus on how terrorists can circumvent this biometric passport system through the use of false breeder document or through acquisition of lost and stolen passports, and how we can better make use of all available information from our databases about known or suspected terrorists.

In short, we need to clarify what the goal is that we are trying to achieve: Are we merely trying to verify that the person to whom the official travel document was issued is the same person who is using the document to gain entry into the United States? Or are we seeking to deploy a comprehensive border security system, which begins at the time the travel document is created and issued? I believe that we should be moving towards an international system, based on biometrics, that screens people before they obtain travel documents, so that we verify people are who they say they are, and ensure that they are not suspected terrorists or criminals.

I am pleased to hear that the Department of Homeland Security recognizes that this biometric requirement for VWP country passports is the starting point, and not the ending point, of this important discussion on how to combat terrorist travel. Both these passports and our own U.S. passports will be equipped with computerized "chips" that are able to accommodate additional biometric identifiers, such as fingerprints. I look forward to hearing from the Department of Homeland Security about its vision of border security through the use of biometric technology, and how these passport requirements can ultimately be integrated with other programs aiming to achieve the similar goal of ensuring secure and efficient travel both within and across U.S. borders—programs such as NEXUS, FAST, SENTRI, TWIC, and Registered Traveler.

I also am pleased that the Department does not intend to change its policy that VWP travelers must enroll in US–VISIT when they arrive at U.S. ports of entry. This program affords us the opportunity to check travelers' fingerprints against available databases to help determine if the person has a terrorist connection, or otherwise has violated U.S. criminal or immigration laws. If VWP passports were encoded with fingerprints, we also would be able to match, with much greater precision, the identity of such passport holders to the person to whom the travel document was originally issued. I hope we can explore this and other issues during today's hearing.

I again want to thank our witnesses and I yield back the balance of my time.

Mr. LUNGREN. The Chair would now recognize the ranking member of the full committee, the gentleman from Mississippi, Mr. Thompson, for any statement he might make.

Mr. THOMPSON. Thank you very much, Mr. Chairman and Ranking Member.

I would like to also welcome our witnesses for this hearing today and associate myself with the chairman of the full committee's comments apologizing for the size of the room. I am sure we will work on that at some point.

Mr. LUNGREN. We will. And I just might say we looked diligently to find a room that Mr. Dicks had never seen since he came with the building and we did find it.

[Laughter.]

Mr. THOMPSON. Thank you very much. I am pleased that the Department of Homeland Security is here to brief us on the status of the biometric passport requirements for the Visa Waiver Program.

Congress has directed the Homeland Security Department to work with the State Department to ensure that visa waiver countries add biometric identifiers to their passport system. Last week, however, DHS announced that it would give the 27 countries participating in the Visa Waiver Program another year to fully implement biometrics. I am concerned about this deadline extension and am hopeful that the witnesses today can explain in more detail why it was necessary.

I ask this because in my experience when you keep pushing out deadlines, it is harder to be taken seriously. When I start to think about all the deadlines the Department has missed or moved, I feel like I am waiting for the cable guy to install my cable between the hours of noon and 5.

[Laughter.]

You do not know when he is coming, if he is coming or how many times you are going to have to call to get service. It is hard to tell when deadlines legitimately need to be extended and when the Department is just dropping the ball.

I look forward to hearing any clarification as to how this extension may be different. At the same time, I understand that we need to make sure that we get biometric passports right.

Last year, the DHS Inspector General issued a report that concluded that aliens applying for admission to the U.S. using stolen passports have little reason to fear being caught and are usually admitted into the country. This is simply unacceptable in the post–9/11 environment.

There are a number of basic questions I look forward to having answered here today. Namely, on the resource side, do we have adequate infrastructure to implement a machine-readable biometric passport system?

On the technology side, do we have a plan to make the various machines readable and biometric tools interoperable?

On the privacy and security side, can we ensure that passengers' biometric information stored on a chip in a passport cannot be improperly scanned by terrorists or other criminals. There is enough identity theft issues we are dealing with these days in the U.S. The U.S. government should not be increasing the odds on this.

On the big picture side, how much more security are we getting with the biometric passports if we are not checking passengers until they are already in flight to the U.S.?

That is a real question, Mr. Chairman. It has been raised in a couple of statements by others, and I look forward to the answer, and I look forward to the testimony.

Mr. LUNGREN. Thank you, Mr. Thompson.

Other members of the committee are reminded that their statements may be submitted for the record.

I ask unanimous consent that the gentlelady from the Virgin Islands, Dr. Christensen, who is not a member of this subcommittee but a member of the full committee, be able to participate in today's hearing, without objection.

We are pleased to have two distinguished panels of witnesses before us today on this important topic.

Let me just remind the witnesses that your entire written statement will appear in the record. We ask that due to the number of witnesses on our panels today, you strive to limit your oral testimony to no more than 5 minutes. We will also allow each panel to testify before questioning any of the witnesses.

I would like to now call the first panel and recognize Ms. Elaine Dezenski, the Acting Assistant Secretary of the Border and Transportation Security Directorate for the Department of Homeland Security to testify.

STATEMENT OF ELAINE DEZENSKI, ACTING ASSISTANT SECRETARY OF THE BORDER AND TRANSPORT

Ms. DEZENSKI. Thank you very much.

Chairman Lungren, Ranking Member Sanchez, other distinguished members of the committee and subcommittee, I am very pleased to be here today to talk about the Visa Waiver Program biometric requirements and the broader vision within the Department for the use of biometrics.

As you know, DHS is charged with the responsibility of securing our travel infrastructure and preserving the integrity of our borders. While at the same time, we need to keep the flow of legitimate travel and trade moving as efficiently as possible.

In executing this mandate, we are always mindful to keep an appropriate balance between these two goals.

Biometrics in particular play a critical role in managing this process. Within DHS, we are using biometrics to strengthen the integrity of travel documents, to verify identity as part of our entry and exit process and to assist with access, control and ID as part of our Transportation Worker Identity Program. These are but a few examples of how we are using biometrics.

Today, I would like to talk just a bit more about our commitment to requiring biometrics in passports and specifically within the context of the VWP program.

Last week, Secretary Chertoff announced a policy directive that clarifies the passport requirements for countries participating in the VWP. VWP allows for visa-free travel for citizens of 27 countries around the world. The policy ensures that the standards for biometric requirements, as set forth in the Enhanced Border Security Act of 2002, are clearly understood and adhered to by all coun-

tries in this program and that our security goals are met as quickly as possible.

Under the policy, VWP countries will be required to adopt specific security and biometric standards. First, VWP travelers must be in possession of passports that are machine-readable. This requirement goes into full effect this coming Sunday, June 26. A machine-readable strip on a passport is absolutely critical to ensuring that the biographic data in the passport can be confirmed as legitimate.

The second requirement is the incorporation of a digital photograph into the data page of passports issued by VWP countries on or after October 26, 2005. Now, why is this important? It is important because a digital photo incorporated into the data page greatly reduces the likelihood of tampering with that photo.

Our announcement last week also called on VWP countries to present a plan by October of this year outlining how they will produce what we refer to as the e-passport, one that contains an embedded, contactless, integrated circuit chip that stores both biographic information as well as biometric information, in this case which would be the digital photo. The chip allows us to electronically authenticate both biometric and biographic data associated with the travel document. VWP countries must achieve full implementation of these e-passport requirements no later than October of 2006.

Now, in addition to these enhancements, we are also requiring VWP countries to help us tackle the important problem of lost and stolen passports. Many of these make their way to the black market and could end up in the hands of terrorists, and, certainly, this is something we need to stop.

A condition of membership in VWP includes the reporting of lost and stolen passports to INTERPOL and to DHS no later than 10 days after discovery. Most times it happens much sooner than that. Also, we are requiring countries to share with us any information they have on trends related to lost and stolen passports.

One of the byproducts of the development of this e-passport policy is a unique international collaboration that continues to grow. Through ICAO, the International Civil Aviation Organization, we have been working with VWP countries over the last couple years to test and perfect technical requirements that will ultimately make it possible for e-passports to be interoperable with our readers at ports of entry.

As Secretary Chertoff announced last week, we anticipate full deployment of our readers by October 2006, which is consistent with the full implementation of the e-passport requirements for VWP countries. As part of this development process, DHS will host a technical conference this summer with all VWP countries and ICAO to address technical and interoperability issues that remain.

Beyond VWP, DHS is pursing biometrics on many fronts. One of the most important efforts is the expansion of the so-called Registered Traveler concept that I think was mentioned a bit earlier by the chairman. We believe there is significant opportunity to develop a RT-type card that could be used in multiple ports of entry and would serve in lieu of a passport at land borders where we are

facing implementation of the Western Hemisphere travel requirements.

We envision this card as being the same size as a driver's license, linked to a background check and with biometric capabilities, such as the contactless chip. I brought with me a sample of our Registered Traveler card which is currently being piloted in the U.S. It gives you an idea of what this card could look like and what we are already producing as part of that pilot.

Again, thank you for the opportunity to be here today, and I look forward to addressing your questions on this important topic. Thank you.

[The statement of Ms. Dezenski follows:]

PREPARED STATEMENT OF ELAINE DEZENSKI

Chairman Lungren, Ranking Member Sanchez and other distinguished Members of the Subcommittee, it is a pleasure to appear before you today to discuss the approach that the Department of Homeland Security (DHS) is taking in our efforts to improve the security of the United States by the use of biometrics in travel documents.

DHS is committed to secure travel and our recent decision to clarify the deadline for Visa Waiver Program (VWP) countries to produce "e-passports" is emblematic of how the Department and the State Department (DOS) are working to keep our borders safe but open for legitimate travelers.

Programs such as the VWP advance our shared goals of protecting travel and preserving the integrity of our borders—while stopping terrorists and those who mean us harm. DHS is committed to continuing the VWP while strengthening it by closing down vulnerabilities such as fraudulent passport use. One means to do this is through the requirement that biometric information be incorporated into travel documents.

Biometrics are the way forward in enhancing security by helping us to deprive potential terrorists of a tool they use to threaten our country and other countries around the world: the ability to cross our borders using false documents and violate our immigration laws without detection. Biometric identifiers protect our visitors by making it extremely difficult for anyone else to assume their identities should their travel documents be stolen or duplicated. The use of biometric identifiers gives governments an increased security capability and a foundation it can build on over time. Properly used, biometrics have been shown to be highly effective in verifying identity.

The U.S. Congress mandated in the Enhanced Border Security and Visa Entry Reform Act of 2002, as amended, that any passport issued on or after October 26, 2005, and used for VWP travel to the United States, must incorporate biometric identifiers that meet internationally accepted standards established by ICAO. The Administration's recently announced policy furthers the intent of the statute by providing for the adoption of biometrics and strengthening the overall management of this important program.

More specifically, we, in consultation with Congress and the Department of State, have established policy that requires VWP countries to begin producing machine-readable passports with digital photographs on the passport's data page by October 26, 2005. Digital photographs provide more security against counterfeiting than traditional photographs. Digital photos can be electronically stored and accessed, making it easier to verify whether the individual currently presenting the passport is the same person to whom the passport was issued. In addition, DHS has established a policy requiring all VWP countries to produce passports with an integrated circuit chip, known as *"e-passports,"* capable of storing biographic information from the data page of a passport, a digitized photograph, and other biometric information no later than October 26, 2006. This information will allow us to achieve a new level of identity authentication.

The effect of this policy is that VWP countries will be required to issue passports that have at a minimum a digital photo by this October and that a VWP traveler to the United States must present a machine-readable passport which includes a digital photograph to enter the United States. These requirements apply only to passports issued on or after October 26, 2005. Valid passports issued before October 26, 2005, will still be valid for travel under the VWP, provided that they are ma-

chine-readable. We believe the vast majority of the VWP nations will be in compliance with the digital photo requirement by October.

The Department recognizes that some countries are very close or have even launched their production of *"e-passports.* Obviously, those countries will also be in compliance with the upcoming deadline. In order to facilitate compliance with e-passport requirements, we will work with each country on a bi-lateral basis with regard to biometrics as well as other security provisions required of VWP countries. Further, DHS will create a validation process for VWP countries to test their biometric passports prior to issuance. In support of this effort, DHS will host a technical conference this summer to address interoperability issues with reader technology and with U.S. passport technology. DOS is leading the U.S. effort in production of e-passport for our own citizens.

In further steps forward on *"e-passports,"* DHS and DOS are conducting a "live test" with the governments of Australia and New Zealand. The "live test" began last week at Los Angeles International Airport and at the Sydney Airport in Australia, and will continue throughout the summer. Airline crew and officials from United Airlines, Air New Zealand and Qantas Airlines have volunteered to use the e-passport when arriving at either airport. Their participation will enable DHS to further test operations, equipment and software needed to read and verify the information contained in an e-passport.

Finally, VWP countries will be held to several measures concerning lost and stolen passports such as—reporting all lost and stolen passports to INTERPOL and DHS, as quickly as possible; sharing information on trends and analysis of lost and stolen passports; and providing detailed information on passport security features.

The progress made toward the *"e-passport"* is a milestone in our global path to secure and streamlined travel for VWP nationals. We appreciate the cooperation of our international partners and the effort they have put forth in this very serious matter.

Mr. Chairman and Members of the Subcommittee, I want to thank you for the opportunity to present this testimony today. I would be pleased to respond to any questions that you might have at this time.

Mr. LUNGREN. Thank you, Ms. Dezenski.

The Chair would now recognize Mr. Frank Moss, Deputy Assistant Secretary of Consular Affairs for the Department of State, for his testimony.

STATEMENT OF FRANK MOSS, DEPUTY ASSISTANT SECURITY OF CONSULAR AFFAIRS, DEPARTMENT OF STATE

Mr. MOSS. Good morning, Chairman Cox, Chairman Lungren, Ranking Member Sanchez, distinguished members of the committee.

Good morning. I am pleased to be here today to discuss the efforts of the Department of State to introduce biometric elements into the U.S. passport, arguably the most valuable identity and citizenship document in the world. Without question, biometrics will strengthen U.S. border security by ensuring that the person carrying a U.S. passport is the person to whom the passport was issued.

The United States adopted the facial image as the first generation of passport biometric identifiers. Our new passport includes a contactless chip in the rear cover that will contain the same data as that found on the biographic data page, including a digital image of the photograph. Looking to the future, we decided to require 64 kilobytes of writable memory on the contactless chip in the event that we subsequently decide to include additional biometrics. Should we decide to change the biometric requirements, we will, of course, vet this change through the Federal Register process.

We are aware of concerns that data written to the contactless chip may be susceptible to unauthorized reading. Several members

of the subcommittee have mentioned that this morning. To help reduce this risk, we will include anti-skimming materials that prevent the chip from being read when the passport is closed or mostly closed. We are also engaged with technical experts in the private sector and our colleagues from the National Institute of Standards and Technology, both to assess the risk of unauthorized reading, and to evaluate the efficacy of our countermeasures.

Finally, we are seriously considering adopting a technical process called Basic Access Control, to strengthen further the defenses of the U.S. passport against unauthorized reading.

The bottom line is that the State Department will not issue biometric passports to the general public until we have successfully addressed these concerns.

In addition to biometrics, two other aspects of the Department of State's passport program enhance U.S. national security: The adjudication process itself and the security features of the passport. By making certain that U.S. passports are only issued to American citizens, that they are more difficult to counterfeit, and that the bearer of the passport is the same person to whom the passport was issued, we are actively enhancing the security of this nation.

Increased information sharing is one of the most effective ways of securing the adjudication process. We have long-standing and effective data share programs with federal law enforcement agencies that target passport applicants of particular concern. Currently, there are nearly 50,000 names of fugitives or other individuals of interest to law enforcement in the passport lookout system. We are working to add to our lookout system an extract of FBI fugitive warrants from the NCIC wanted persons file.

We also have an agreement with INTERPOL that allows us to share information about approximately 620,000 lost and stolen U.S. passport with INTERPOL member states. We have also implemented a cooperative relationship with the National Counterterrorism Center, NCTC, to provide that agency with direct online access to our database that includes images of the passport application for all valid passports. And we will also sign in the very near future an agreement with the Terrorist Screening Center that will add to our database information on American citizens who may have a nexus to terrorism.

We have also undertaken a comprehensive review of our fraud prevention efforts to strengthen that aspect of the adjudication process. We have implemented a number of initiatives, including organizational improvements, enhanced training, regulatory changes, new tools and new programmatic activities with domestic and international partners.

We enjoy excellent cooperation and support from the Bureau of Diplomatic Security at the Department of State, which has the responsibility for criminal investigations involving passport fraud, and our focus on fraud prevention is already paying dividends. So far in fiscal year 2005, Diplomatic Security has opened over 2,400 passport investigations and made nearly 400 arrests, a significant increase over prior years.

We have recently completed the first cover-to-cover redesign of the United States passport in more than a decade in order to combat counterfeiting or the fraudulent use of lost or stolen passports.

The passport includes a host of advance security features, including sophisticated new artwork, printing techniques used in the current generation of U.S. currency, and utilizing a variety of other techniques, many of which are visible only under ultraviolet light.

I am happy to share with members of the committee samples of the new passport, and my written testimony includes additional elements about the enhanced technology we used to create it.

To put the scope of our efforts in context, during the last fiscal year, the Department of State processed a record-setting 8.8 million U.S. passport applications. Passport demand continues to rise and we are track to adjudicate more than 10 million passports by the end of this fiscal year.

Taking into account recent legislation concerning the documentary requirements for travel within the Western Hemisphere, we anticipate that passport applications will total about 12 million in fiscal year 2006. Projections beyond that date are admittedly less precise, but we are currently planning that U.S. passport demand will reach about 14 million in fiscal year 2007 and an estimated 17 million by 2008.

Security must always be our first priority, but we must also recognize our responsibility to adjudicate passport applications in a timely and efficient manner to facilitate the travel of U.S. citizens. The free movement of people and goods is essential to U.S. national security, as is our international engagements through personal, commercial, educational and research activities with other nations.

Mr. Chairman, integrating biometrics into U.S. passports will further protect the integrity of the world's most respected travel document. Together with our improvements to the adjudication process and the physical security of the passport itself, the Department's comprehensive passport program serves to enhance U.S. border security.

At this time, I am happy to answer your questions. Thank you very much.

[The statement of Mr. Moss follows:]

PREPARED STATEMENT OF FRANK E. MOSS

Chairman Lungren, Ranking Member Sanchez, Distinguished Members of the Subcommittee:

I am pleased to have this opportunity to discuss with you the progress that the Department of State has made in introducing biometric elements to the U.S. passport. This innovation represents a significant enhancement to the security of our borders and international travel. In addition to the inclusion of biometrics in U.S. passports, two other aspects of the Department of State's passport program are critical to enhancing U.S. national security: the adjudication process, and the security features of the passport itself. Taken together, these elements constitute a comprehensive approach to passport security. By making sure that U.S. passports are only issued to American citizens, that they are more difficult to counterfeit and that the bearer of the passport is the same person to whom the passport was issued, the Department of State actively enhances the security of this nation.

Today I would like to describe the many ways that the Department of State demonstrates its commitment to the important responsibility for providing passport services. The U.S. passport is arguably the most valuable identity and citizenship document in the world. We at the Department of State are certainly aware of how sought after this document is, not only by American citizens with legitimate travel plans but by illegal immigrants, as well as terrorists and others who would do this nation harm. As portable proof of identity and nationality, the U.S. passport literally opens doors around the world to American citizens who travel or reside abroad or may require assistance from an American Embassy or Consulate. The

U.S. passport is also essential for many American citizens to enter the United States upon returning from international travel.

During the last fiscal year the Department of State processed 8.8 million U.S. passport applications. This set a record, exceeding the total from the previous year by more than one million applications and representing a workload increase of some 22 percent. This year, the Department of State forecast a 9 percent increase in passport demand, but is experiencing a 14 percent rise. As of today, the Department has already processed close to 7 million passport applications during this fiscal year and we are on track to adjudicate more than 10 million passports by the end of fiscal year 2005.

The Intelligence Reform and Terrorism Prevention Act of 2004 also contains a provision addressing the documentary requirements for travel within the Western Hemisphere, referred to as the Western Hemisphere Travel Initiative (WHTI). The legislation requires that the Secretary of Homeland Security, in consultation with the Secretary of State, develop and implement by January 1, 2008 a plan to require U.S. citizens and non-U.S. citizens currently exempt from presenting a passport for travel within the Western Hemisphere to present a passport or other authorized documentation that denotes identity and citizenship when entering the United States. The Department of State, after analyzing the scope of WHTI and other projected growth in passport demand, expects that applications for passports will total about 12 million in FY-2006, about 14 million in FY-2007 and reach a potentially sustainable annual demand of 17 million by FY-2008.

As the Department of State develops plans to address the increase in demand for U.S. passports resulting from normal growth in international travel and the WHTI, we are dedicated to ensuring that security vulnerabilities are not inadvertently created by our efforts to address the increase in workload. While keeping security imperatives in mind, the Department of State also recognizes its responsibility to adjudicate passport applications in a timely and efficient manner to facilitate the travel of U.S. citizens. The free movement of people and goods is essential to U.S. national security, as is our international engagement through personal, commercial, educational and research activities with other nations. We are actively pursuing initiatives to improve the U.S. passport program designed to support both of these objectives.

Strengthening the Adjudicatory Process

A key objective of the Department of State's Office of Passport Services in the Bureau of Consular Affairs is to ensure that U.S. passports are issued only to persons who are legitimately entitled to them. This is particularly important in an era when terrorists, transnational criminals and others seeking to enter the U.S. illegally view travel documents as valuable tools, and when improvements to the physical security of the U.S. passport, such as the use of a digital photograph of the bearer, make it increasingly difficult to counterfeit.

One of the most effective ways to ensure that only those entitled to U.S. citizenship receive a passport is increased information sharing, both within the United States Government and beyond. The Department of State has actively worked to establish data exchange programs with other agencies in a manner that is mutually beneficial and that will keep U.S. passports out of the hands of those who are not eligible to receive them. For example, the Department has a partnership with the Department of Health and Human Services (HHS) that ensures that parents with child support arrearages, who are ineligible to receive passports, do not receive them. The incorporation of over 3 million names in the HHS database into the Department's passport lookout system has also resulted in the recovery of more than $50 million in delinquent child support.

In April 2004, the Department signed a memorandum of understanding with the Social Security Administration (SSA) that would permit the Department to verify the SSNs of U.S. passport applicants with information in SSA's SSN database. This measure provides another verification tool for passport specialists and consular officials adjudicating passport applications by allowing them to correlate the data provided by a passport applicant with information in SSA's system and use this information to support decisions about an applicant's identity.

The Department has a long-standing and effective working relationship with federal law enforcement agencies that targets passport applicants of particular concern. Today, we have nearly 50,000 names of fugitives or other individuals of interest to law enforcement in the passport lookout system. Half of these were entered individually as a result of our outreach efforts. The other half of these entries are based on U.S. Marshals Service (USMS) federal fugitive warrants, a process that the Department took the initiative to obtain.

To complement the USMS information, work is well underway to add to the passport lookout system an extract of FBI fugitive warrants from the NCIC Wanted Person File. To encourage information exchange with law enforcement officials at the state and local levels, the Assistant Secretary of State for Consular Affairs wrote to all the states' attorneys general.

In 2004, the Department reached an agreement with INTERPOL to provide the Department's lost and stolen passport database to the U.S. National Central Bureau (NCB). The NCB shares the data with INTERPOL, which in turn makes this information available to all INTERPOL member states. The U.S. lost and stolen passport database currently contains the passport numbers of over 620,000 passports.

The Department's Office of Passport Services is also currently working on an agreement with the Terrorist Screening Center that would provide information on American citizens who are either subject to a federal felony arrest warrant or who are considered persons of concern due to a nexus to terrorism or an ongoing investigation. This datashare program will enable the Terrorist Screening Center to learn of the passport application of an individual of interest and, under appropriate circumstances, take law enforcement action.

In addition, the Department's Bureau of Consular Affairs has implemented a cooperative relationship with the National Counter Terrorism Center (NCTC) to provide that organization with direct online access to the Passport Records Imaging System Management (PRISM). This database includes images of the passport applications for all valid passports. The NCTC utilizes this information as a verification tool to support its terrorist watch list responsibilities.

Another important element in safeguarding the adjudicatory process is maintaining an aggressive fraud prevention program. In that regard, the Department of State has undertaken a comprehensive review of its fraud prevention efforts and implemented a number of initiatives, including organizational improvements, enhanced training, regulatory changes, new tools, and new programmatic activities with domestic and international partners. All senior passport specialists now rotate through the fraud prevention office at domestic passport facilities to give them specialized experience in fraud detection. Regulatory changes have been implemented, for example, to require that both parents consent to the issuance of a passport for a child, and to require the presence of children under the age of 14 when passport applications are executed on their behalf, in order to combat fraud and international parental child abduction. We are making greater use, with the appropriate respect for privacy concerns, of commercial databases to assure that persons applying for passports are who they claim to be.

The focus on fraud prevention is already paying dividends. Statistics for this fiscal year show an increase in referrals to fraud prevention offices, as well as an increase in the referral of presumptive fraud cases to the Department's Bureau of Diplomatic Security (DS) for further investigation. The Bureau of Consular Affairs enjoys excellent cooperation and support from DS, which has the responsibility for criminal investigations involving passport fraud. The statistics about the efficacy of joint Consular Affairs-Diplomatic Security efforts are compelling: so far in fiscal year 2005, DS opened 2401 passport investigations and made 375 arrests, a significant increase over previous years.

Redesigning the Passport

Efforts to strengthen the adjudication process and augment fraud prevention efforts would be less effective if we did not attend to the other key elements of passport security with equal fervor. Turning to the passport itself, the Department recently completed the first cover-to-cover redesign of the document in more than a decade. The new passport includes a host of new security features, including sophisticated new artwork, adopting printing techniques used in the current generation of U.S. currency, and utilizing a variety of other techniques, many of which are only visible under ultraviolet light.

Our objective in designing the new passport is to raise further the bar against counterfeiting or the fraudulent use of lost or stolen passports. Advances including color shifting ink, microprinting, latent image lettering and a security laminate over the biographic data page that includes optical variations, all serve to deter counterfeiters and forgers. The biographic data page has been relocated from the inside of the front cover to the first inside page for added security. The inventory control number for each book is now the same as the passport number. Imagery on the inside pages of the passport incorporates more colors, stylized depictions of iconic American scenes, and includes famous quotations from American history. The new passport, combined with security enhancements in the adjudication process, helps to ensure that only qualified applicants receive U.S. passports.

I am happy to share with the members of the Subcommittee samples of the new passport.

Beyond the physical content of the book itself, we scrutinize each step in the production and delivery process to eliminate vulnerabilities. In addition to improving the quality of the U.S. passport, the Department of State, building on an already excellent collaboration with the Government Printing Office (GPO), is working to secure further the delivery of blank passport books to domestic passport facilities by engaging armored truck service. This mode of delivery service is used by the Department of Treasury to move currency and other valuable documents around the country.

Biometrics

This next generation of U.S. passport, the e-passport, includes biometric technology that will further support the Department's border security goals. Without question, biometrics will strengthen U.S. border security by ensuring that the person carrying a U.S. passport is the person to whom the Department of State issued that passport.

Consistent with globally interoperable biometric specifications adopted by the International Civil Aviation Organization (ICAO) in May 2003, the United States has adopted the facial image as the first generation of biometric identifiers. The new U.S. passport includes a contactless chip in the rear cover of the passport that will contain the same data as that found on the biographic data page of the passport, including a digital image of the bearer's photograph. This data includes the following information about the bearer: the photograph, the name, the date and place of birth, as well as the passport number and the date of issuance and expiration. Looking to the future, the Department decided to require 64 KB of writeable memory on the contactless chip in the event that we subsequently decide to introduce additional biometrics. Should the United States Government decide to change the biometric requirements, this change will be subject to vetting through the Federal Register process.

On June 15, the Department, partnering with the Department of Homeland Security and in collaboration with Australia and New Zealand, launched an operational field test to measure the overall performance of the e-passport, issuing approximately 250 U.S. e-passports to select airline personnel employed by United Air Lines and who fly from Los Angeles to Australia and New Zealand. The Department of Homeland Security has developed separate lanes and installed e-passport readers to test their efficiency. Later this year we will expand this pilot program to include diplomatic and official passports, with national deployment of the e-passport scheduled for 2006.

The Department of State is well aware of concerns that data written to the contactless chip in the e-passport may be susceptible to unauthorized reading. To help reduce this risk, anti-skimming materials that prevent the chip from being read when the passport book is closed or mostly closed will be placed in the passport.

The Department is also seriously considering the adoption of Basic Access Control (BAC) technology to further strengthen the privacy of the data contained on the chip. ICAO recently identified BAC technology as a "best practice" for passport security. BAC technology will prevent the chip from being read until the passport is opened and its machine-readable zone is read electronically. This will serve to "unlock" the chip and permit the chip and reader to communicate through an encrypted session. We are engaged with technical experts from the private sector and the National Institute of Standards and Technology both to assess the risk of unauthorized reading and to evaluate the efficacy of countermeasures. **The bottom line is that we will not issue biometric passports to the general public until we have successfully addressed these concerns.**

The Department is confident that the new e-passport, including biometrics and other improvements, will take security and travel facilitation to a new level. Naturally, the Department will test comprehensively the operation and durability of the e-passport and work to resolve any issues as they occur. In fact, the Department of State is engaged in a continuous product improvement effort with regard to the U.S. passport. We will continue to monitor technical developments and help conduct research to ensure that we produce a passport that is highly secure, tamper resistant and globally interoperable.

Mr. Chairman, I am grateful for the opportunity today to share with you the Department of State's comprehensive approach to enhancing U.S. border security by augmenting the security of all aspects of the U.S. passport program. The introduction of biometrics is an important advance in continuing to protect the integrity of the world's most respected travel document. At this time I am happy to answer any

questions you, the Ranking Member and the other distinguished members of the Subcommittee might have about the Department's biometric passport program or the other facets of the U.S. passport program that I have discussed.

Mr. LUNGREN. Thank you both for your testimony, and I will recognize myself for 5 minutes to begin the questions.

Mr. Moss, what was the number you gave of lost and stolen U.S. passports?

Mr. MOSS. We have provided INTERPOL information on about 620,000 lost U.S. or stolen passports. This is several years' worth of data, and that has to be compared, I would suggest, to the fact that we have roughly 63 million U.S. passports in circulation.

Mr. LUNGREN. I guess I should know this but I do not. Is there any legal obligation on the bearer of the passport to report within a period of time if it is stolen or lost?

Mr. MOSS. There is no legal obligation. When we find out that most people have reported their passport stolen, it is either they realize it and tell us promptly or they go to use it, realize it is lost and then come to us. The other aspect, of course, is that people do lose their passports while traveling abroad, and we have processes to replace those rather quickly.

Mr. LUNGREN. Do we have any estimate of how many are stolen or lost that we do not know about? I mean, is there any idea, estimate or study?

Mr. MOSS. I think we are dealing with one of the intangibles, what we do not know, we do not know.

Mr. LUNGREN. Right.

Mr. MOSS. I would not even want to hazard a guess, really, sir.

Mr. LUNGREN. Given that the fingerprint technology and fingerprint databases are much more readily available, that they are the cornerstone of our main border screening system, the US–VISIT Program, and that many other countries have that biometric, can each of you describe why the U.S. and ICAO chose facial recognition rather than fingerprint as the biometric standard for official travel documents?

Ms. DEZENSKI. Sure. There are a couple key reasons. The first is that from a cultural and even from somewhat of a political perspective, the facial image is something that most people do not have privacy concerns over. It is much easier to obtain across the board when we are looking at documents like passports and visas.

But it is important to keep in mind that even though the passport may not have fingerprints, we are using fingerprints as part of the enrollment process for both US–VISIT and of course to obtain a visa. So there is a visa biometric that involves fingerprints and utilizes those databases in the process of admitting foreigners to the U.S.

Mr. LUNGREN. But the fingerprints are not part of the passport document itself.

Ms. DEZENSKI. That is correct.

Mr. LUNGREN. And you suggest that that is, I do not want to put words in your mouth, but my understanding of what you just said is that it is culturally difficult or politically difficult for us to get acceptance of fingerprints. Yet 9/11 changed the world.

And if we are serious about the terrorist threat, it seems to me we ought to be moving in the direction of that biometric which is

going to most protect us. Perhaps what we ought to be doing is explaining that this is a superior biometric to at least any other that I am aware of, both because of the accuracy with which it conveys information and the universality of fingerprints as the identifier for various databases, particularly those that would, I assume, be the basis for watch lists of all sorts.

How do both of you, or your departments, view the essential difference in degree of efficacy in the facial recognition versus the fingerprint identification?

Ms. DEZENSKI. We do think there is value in the use of the digital image. I think it is important to put into context that when we talk about the biometrics features of the passport, it is going to an ICAO requirement or an ICAO recommended process, if you will, which has gone through a process via the international community. So there was actually a tremendous amount of discussion about what could be adopted in the short term, what would be the most efficient and what would allow us to get to the standard with the biometrics that many countries could work with.

I think I would again emphasize that when it comes to our own processes, US–VISIT, for example, we are in fact using the biometric fingerprint process, and we feel that that is very important to ensure that we can check against relevant databases. The use of the biometric digital image in the passport, as part of the data page, which is what I defined as one of the requirements in the VWP Program, is, first and foremost, about being able to detect tampering with that document. If the digital photo is part of the data page, which is in fact our requirement, it is much more difficult to carve out that picture, affix a new picture, or otherwise tamper with the document.

Ms. LOFGREN. So goes the tamperproof nature of the document as opposed to me really knowing whether the person in front of me is the person he or she says he or she is.

Ms. DEZENSKI. Well, that is the first point. The second point is that we need to link up that digital photo to the integrated circuit chip. Through the integrated circuit chip, we are actually able to write that biometric information within the passport along with the biograph data in the cover page, on data pages of the passport, and we can do a check to ensure that the person standing in front of us is in fact the same person whose image is coming up now on the screen in front of the inspector.

So there is that link, and we do think that that gives us an added layer of security.

Mr. LUNGREN. I have got a lot more questions, but my time is expired.

The gentlelady is recognized.

Ms. SANCHEZ. Thanks, Mr. Chairman, although you are the chairman, so if you—

Mr. LUNGREN. We are going to have a lot questions here.

Ms. SANCHEZ. We all have a lot of questions.

I am looking at the passport you are passing around. Do you have chips in these or are we just pretending?

Mr. MOSS. No, Congresswoman, those passports have a chip embedded in the rear cover, and in fact the data that has been written to the data page has been copied to that chip. The chip is very

small. Look at the passport you are holding, and turn to the passport's to the rear cover, it is in the upper left—I have got to think my own geography here—it is in the upper left corner.

It is very, very small. It is approximately an eighth of an inch, [perhaps an eighth of an inch] square plus the antenna. It is designed to be small even though it contains a great deal of data so that it is not obvious to the individual.

Ms. SANCHEZ. Okay. We just wondered.

Mr. LUNGREN. Now it is.

[Laughter.]

Mr. MOSS. Sir, we are not making it secret. We just do not want it to be bulging out of the back, if you would.

Ms. SANCHEZ. That technology, do you think it will last for the 10 years of the issuance of the passport? Because, I mean, my passport goes in the back of my jeans, through the washing machine and God knows what else.

Mr. MOSS. I guess the first point I would make is that passports and water do not mix well, nor do electronic passports, water and chips mix well. The point, though, about overall durability, is that we have actually contacted with our colleagues at the National Institute of Standards and Technology to do extensive testing on the new passport, including looking at the issue of chip durability. That is one of the key factors as we assess proposals from vendors. We are certainly looking for a 10-year chip and the industry assures us that the chips will last for 10 years. We believe in "trust but verify". That is why we have hired NIST to help us do that.

Ms. SANCHEZ. I have several other questions. The last one I have for you is these 600,000 passports that are missing in action. Are those invalidated? Do we keep a list? Can I come use my—

Mr. MOSS. We have actually changed our regulatory practice so that once you report a passport as being lost or stolen, it is invalid for international travel. We report it to INTERPOL, we share that data with our colleagues at the Department of Homeland Security, and I strongly urge anyone who loses a passport and then finds it and has reported it to the State Department, not to travel on it. It may not be a pleasant experience.

But, yes, it is an invalid travel document.

Ms. SANCHEZ. And to the Department of Homeland Security, this subcommittee has held on the Registered Traveler Program, and the estimate from the Department put the potential membership in that program might be up to 4 million United States travelers. TSA has yet to decide whether it is going to continue the program or what it is really going to look like. We just spent some time with them these past 2 weeks.

However, it is my understanding that the Department is considering using the biometric registered travel card as an alternative to passports required under the Western Hemisphere travel initiative; is that correct?

Ms. DEZENSKI. No. Actually, that is not the case. We are looking at a RT-type concept as part of the solution to meet the Western Hemisphere travel requirements, but we have not made a decision that the current RT pilot programs and the card that we are issuing as part of those pilot programs would be an acceptable form of identification and citizenship validation to meet the Western

Hemisphere requirements. So I think we just need to make that distinction here.

We think there are opportunities to take the RT-type concept and expand it to a border management process.

And, Ranking Member Sanchez, you mentioned the SENTRI Program, the NEXUS Program and other programs that we have already that serve somewhat in that capacity, and it is our goal to take those programs and combine them as part of a global enrollment system within the Department.

We want to get a handle on all of our registered travel type programs and link them into a system that is much more uniform and that allows for much more consistency in terms of background checks and requirements and what the card would look like and all those details that are associated with these type of programs.

So when I mentioned that the Registered Traveler-type concept might be applicable, that is the vision that we have.

Ms. SANCHEZ. So you are talking to the other pieces of the Department to make sure that as they are going along on theirs you might have interoperability between everything?

Ms. DEZENSKI. Absolutely. And that is already happening. We have a tremendous amount of activity within the Department mainly involving US–VISIT, Customs and Border Protection and TSA. Those are the three entities that have some piece of the Registered Traveler issue, if you will, and we are already looking at those issues of interoperability.

Ms. SANCHEZ. And then I have a question for both of you. How many places does the State Department currently issue passports? And how many places does DHS currently issue NEXUS, FAST, SENTRI cards, et cetera?

Mr. MOSS. The State Department has over 7,000 passport acceptance facilities around the United States. I should make it clear: They are not our offices but they are post offices, they are clerks of court, offices like this where people can apply for a U.S. passport. We also have 16, soon to be 17, passport agencies that handle essentially walk-in traffic. But the big issue is, we do have these 7,000 agencies. I can actually share with you a list of those in California. I think there are over 600 in California alone.

Mr. LUNGREN. The gentleman from California, Mr. Cox, is recognized for 5 minutes.

Mr. COX. I want to thank you very much, both of you, for your testimony.

We have been passing around up here on the dais some of the sample passports and this Registered Traveler pilot program card, which is also embedded with a chip. And I am struck in the case of the passports in this card and virtually everything else that we have been discussing here this morning with the, in my view, misuse of the term, "biometric," to describe a photograph.

In my view, biometric must include some measurement, that is the whole point. But the way that we are using the digital photograph, at least in the near term, is simply to have a human being, a government employee look at the picture, visually inspect the person who is presenting themselves and try and match the individual with the photograph. That is not a biometric identification,

in my view. This is really no different than the Matthew Brady technology of the U.S. civil war. It is a picture, that is all it is.

The chip, which may serve to frighten people across the country concerned about privacy, is really nothing more than information that could be written out inside the passport. It is data, which is information about the individual, place of birth, presumably, a whole lot of other things that you might seek to include, but there is no mysticism to it. It could be written out and enhanced as well as put on this chip.

So talking about it as a biometric, we are talking about the length between the chip and the picture in a computer. I think masks the fact that there is no biometric identifier that is being used to connect the person to the document. We have to remember why we are here and what the point of all of this is, because it is supposed to be security. The purpose is to connect intelligence about terrorists to terrorist travel. So if a known terrorist were traveling under an unknown alias, we want to be able to stop him anyway.

I am very concerned, Ms. Dezenski, about what you said, it is the first time I have heard the U.S. government say this in an official forum about fingerprints, that somehow facial recognition technology, which measures the bridge of my nose, the distance between my irises or an iris scan, which I have already subjected myself to as part of the Registered Traveler Program, is somehow less intrusive than getting a fingerprint.

I do not think the U.S. government has any information that establishes that, that people believe that it is more intrusive to take a fingerprint than these other kinds of biometric measurements. But if you have data to support what you said, I would certainly like to know about it. Can you tell me what you are relying upon to make that statement?

Ms. DEZENSKI. Certainly. The comments that I made earlier reflected the outcome of the ICAO process. As I mentioned, we have been working very closely with visa waiver countries and with ICAO to move toward the adoption of biometric requirements. And although I was not part of those discussions with ICAO, it is my understanding that in the process of this international collaboration, the decision was made that a biometric digitized photo would in fact meet the requirement of a biometric within the travel document and that that was the preferred biometric.

Mr. COX. That I understand, but you made a different statement which is that in your view there is cultural resistance to the use of a fingerprint as a biometric. What is the basis for stating that?

Ms. DEZENSKI. Again, that is a reflection of the ICAO discussion where many countries came to the table and although in our country we may not have the same concerns about using fingerprints, obtaining fingerprints, providing those fingerprints, it is not necessarily shared with the rest of the world. And oftentimes there is the perception that if you are fingerprinting travelers, it is akin to booking someone on a criminal charge, for example. I mean, these are the kinds of perceptions that are out there in the international environment. I am not saying that that is necessarily what we believe here in the U.S.

Mr. COX. I think you need to be rather methodical about the way we go forward and not say that we simply cannot use biometrics. We are instead going to have a human being look at a picture, the same old rough justice form of identification that has been in use for years. What we do not want is for terrorists to be able to get good government documents because they have got fake breeder documents and they have got ways to essentially secrete themselves in the form of somebody else whose picture looks exactly like them, at least to the naked eye.

If you will indulge me, Mr. Chairman, I will just remind our colleagues of a question that Eleanor Holmes–Norton asked at one of our hearings a few years ago. We were talking about Canadian truck travel across the northern border, and the Canadians had a card like this with a biometric, and we were all excited about the fact that this was going to much more rigorously identify who was coming across the border.

And she asked during the hearing, "At what point do we check the biometric? How does that work? When does the person slide this card through something or whatever to check the biometric?" And the answer came back that only happens if the person in the booth thinks that the driver looks suspicious.

So it was very clear that the lack of a biometric, the human interface, the judgment, the rough justice part of it introduced civil liberties concerns itself so that the crime of driving while looking suspicious turns out to be the way that we drill down into individual suspects rather than just knowing who we are dealing with.

It would actually, in my view, it would be a big improvement from a civil rights, civil liberties standpoint to be able to say, "You are you, we know that," reduce the size of the haystack. A lot of voluntary programs like Registered Traveler can help us do that.

There is ubiquitous technology right now. You can touch your finger to open your laptop. I do not believe there is any cultural resistance to this whatsoever, and I also believe that the ubiquitousness of the fingerprint as an identifier with criminal detective work around the world means that we are going to be able to tap into a lot more useful information if we do that than if we take the fanciest technology that somebody tries to sell us in the form of facial recognition software, what have you.

Thank you for allowing me that extra time, but, Mr. Chairman, I do think that the Department is making the right decision here, but I think that is because I think there is so little security payback from this whole system, even if we get to the intended destination.

Mr. LUNGREN. I thank the gentleman for his comments.

The gentleman from Mississippi, the Ranking Member Thompson, is recognized for 5 minutes.

Mr. THOMPSON. Thank you very much. And I want to take off from the chairman's comments. What if someone steals the chip and puts it on the passport, and have we not altered the biometrics?

Mr. MOSS. Sir, in fact you have not. The technology that is being used is a technology that once the data is written to the chip by the United States or Germany or any other government, that data

is effectively locked down. It can be read thousands of times, it can only be written to the chip once.

And if the data is changed on the chip, we use a technology called [a version of] Public Key Infrastructure, which serves to authenticate that data. Literally, if one bit of data on the chip is changed, it will throw off a mathematical calculation and help to point out to the well-trained border inspector or consular officer at a post abroad looking at the same passport that something had been done to this passport. So just stealing the chip really does not do someone a lot of good.

Mr. THOMPSON. Mr. Dezenski, in May of this year, we had two airlines diverted to Bangor, Maine, and it was said that en route the match on the name list indicated some problem. Why can't we do the match before the plane leaves?

Ms. DEZENSKI. Well, that is exactly where we are heading. You may be familiar with what is called APIS data, Advance Passenger Information, data that we now receive from air carriers about 15 minutes after a flight takes off. It is essentially a manifest that is equivalent to the information on the data page of your passport. So the biographic information that is captured in the passport is generally the same as what is collected by the air carrier and what we call APIS data.

We actually have two rulemakings that are related to this topic. The first was a rule that came out in early April requiring some additional data elements that fall under this category of APIS data. The second rule, which has not yet been released but is in the final coordination period within the Department and with OMB, is our APIS plus rule, which essentially will move that process back so that we are no longer receiving that information 15 minutes after the flight takes off.

Because the rule is not final, I am not at liberty to talk about exactly what the timeframe will be, but I can tell you that we have had pretty intense discussions with the air carriers and other parts of the aviation community about how to get through the technical and operational challenges to receiving that information. Because we are working in pretty much a just-in-time environment within the airport, it is sometimes difficult to get that information well in advance.

We are often asked the question, "Well, what about the information that we receive or could be received at the point of purchase, for example, as a person buys their ticket, is it possible that we could get some of the data from that point onward? And it is very, very difficult to obtain that information from numerous sources if you think about how people buy their tickets these days. So we are really dependent upon the air carrier and when that person is checking in for their flight to get the full complement of APIS data that we need.

Now, sometimes we have passengers that are transferring from other flights. Sometimes we have folks that are diverted, their flight is canceled, whatever the case may be. And so there will always be instances where we do not have all of the APIS data at the point where we would like to. So we are trying to come up with a solution that allows us to get as much of that data as possible, and our intent is to run those checks before that flight leaves so

that we can deal with those potential threats before that flight takes off, and that will obviously help with reducing the number of diversions.

Mr. THOMPSON. So are you now going to put an additional burden on the carriers to get additional information?

Ms. DEZENSKI. There are two pieces. We asked for two or three additional data elements. That regulation already went into effect in April. We think that is fairly straightforward. We have not had a lot of major concerns coming up. The more problematic piece is the timeframe in which we asked for that information, and that is where we have had a lot of negotiations, a lot of discussions with affected parties about the viability of getting that information.

And then, of course, we have to run our checks on that data. So it has to be early enough in the process that we can run it through our system and get the information back to, in this case, the carriers if in fact we do not want to have a particular person board the aircraft.

SUPPLEMENTAL MATERIAL FOR THE RECORD

Question: Can you tell me, what kind of extra data do you ask for? (Page 45, line 1034)

Answer: We ask for the following information: country of residence; passport expiration date, if a passport is required; and address while in the United States (number and street, city, state, and zip code), except that this information is not required for U.S. citizens, lawful permanent residents, crew members, or persons who are in transit to a location outside the United States.

Mr. THOMPSON. Can you tell me, what kind of extra data do you ask for?

Ms. DEZENSKI. I cannot remember all of the elements. One was the destination address in the U.S. That was something we were not collecting beforehand, and we wanted to have a sense for where people were going. There were, I think, two other elements which I would be happy to get for you.

Mr. THOMPSON. How can you prove where somebody is going?

Ms. DEZENSKI. There is no 100 percent guarantee. It is another piece of information that we can add into our equation, but there is never a guarantee.

Mr. THOMPSON. Well, I guess if you are putting the burden on the carrier to give you information that cannot be verified, it just looks like you are putting an additional burden on the carrier.

Ms. DEZENSKI. Well, we believe that the additional data elements will in fact help us make a better risk assessment decision. Again, there is never 100 percent guarantee, but we do need to work with the carriers to get this type of information.

Mr. THOMPSON. If I say I am going to Washington, D.C., and I am staying at the Hyatt on Capitol Hill, how can you verify that? If you are requiring the carrier to give you this information, are you now making the carrier policemen too?

Ms. DEZENSKI. No. In fact, our goal with this APIS process is to take the process of checking information against our watch list in house. Right now, we are asking carriers to do a check against the no-fly list, for example. We want that process within the government. We want to own that process, we need to own that process.

Mr. THOMPSON. Well, I think all of us want the process to be the best possible, but I cannot see the rationale for asking for information that cannot be verified.

Well, lastly, what is the timeline on the rule for APIS Plus?

Ms. DEZENSKI. We are looking probably over the next couple months to get that issued. It is difficult for me to predict with 100 percent certainty, given that we must complete OMB review and go through the final review process. But we are working as quickly as we can to get that out.

Mr. LUNGREN. Thank you.

The gentleman from Georgia, Mr. Linder, is recognized for 5 minutes.

Mr. LINDER. Thank you, Mr. Chairman.

How many other nations use digitized photos on their passports?

Ms. DEZENSKI. Well, certainly, within the VWP Program, the vast majority do. I think about 25 of the 27 countries use digitized photos. Beyond the VWP group of countries, I am not sure.

Mr. MOSS. Digitized photos are widely used around the world. They are utilized by many countries. China uses them, Russia uses them, many others, because they have a tremendous security advantage over physical photographs. They have really eliminated the problem of photo substitution—of literally changing the photograph in the passport.

Mr. LINDER. Are you having a problem with people putting on makeup to make themselves look like the photo in the passport, have you?

Mr. MOSS. No, we have not, but that is of course one of the issues that having the data written to the chip and having the image there will help us with.

Mr. LINDER. How many visitors to our country that do not live here come with a passport from, say, Saudi Arabia with the fingerprints or a digitized photo?

Mr. MOSS. Any visitor from Saudi Arabia will of course require a U.S. visa. They will have been subjected to a thorough screening, including the collection in almost all cases of two fingerprints as part of the visa application process. The State Department then shares that data with our colleagues at the Department of Homeland Security and that data populates the US–VISIT database. And then when that traveler arrives with their Saudi Arabia travel documents, they are verified as being the same person who applied previously for the visa in Jeddah or Riyadh.

Mr. LINDER. By fingerprint.

Mr. MOSS. By fingerprint, yes.

Mr. LINDER. Why don't you do that for everybody?

Mr. MOSS. Well, sir, we in fact do that for all travelers who arrive here using a visa.

Mr. LINDER. But not for American passports.

Mr. MOSS. We do not include finger scans as part of the U.S. passport process.

Mr. LINDER. Why?

Mr. MOSS. The international community has focused on the issue of facial recognition as a globally interoperable biometric. That is what we have selected, I would emphasize,as our first generation biometrics. As we see what happens in terms of biometric stand-

ards and in terms of efficacy, we may make additional decisions. But right now we are looking at facial recognition as our first generation biometric.

Mr. LINDER. Do you disagree with Chairman Cox's definition of biometric?

Mr. MOSS. I never disagree with committee chairmen.

[Laughter.]

I would say, however, that in our experience in other aspects of the visa process where we have actually used facial recognition software in what are called, "One to Many Applications," we have found some very, very impressive results from facial recognition software and its ability to match visa applicants against the same person applying literally using disguises or applying multiple times for the same benefit.

Mr. LINDER. This picture we saw is going to be judged by an individual standing there looking at it, not facial recognition software; is that correct?

Mr. MOSS. I think it is fair to say in the first generation of applications, even at the ports of entry, it will probably be producing on the inspector's screen, first of all, a much larger image. They will no longer be comparing a traveler to a one and a half-inch square photograph. It will be coming up as a large-size photograph. I think it is also fair to say that the Department of Homeland Security, in addition to its reliance on finger scans for US–VISIT, continues to have interest in the possible reliance on facial recognition software. That technology, though, is still evolving, and we will see where it goes over the next couple of years.

Mr. LINDER. Ms. Dezenski, did you see The Washington Post this morning on the US–VISIT Program?

Ms. DEZENSKI. Yes, I did.

Mr. LINDER. Would you care to comment on the name matching

Ms. DEZENSKI. Well, I think it is important to put that article into context. When we talk about 150 crew members that may have had some issues moving through the US–VISIT process, that is a very, very small fraction of the number of people that move through that program on a daily, weekly, yearly basis. We are talking about a very small fraction.

Of the 150, I think, who were identified as having problems, only about half of those had a specific redress issue with the VISIT system. The others were hits on our IBIS database and were referred to secondary for additional screening and clearing, as needed.

Mr. LINDER. With fingerprints?

Ms. DEZENSKI. Some of them were, yes. I do not know the specifics of any other cases.

Mr. LUNGREN. Mr. Dicks is recognized for 5 minutes.

Mr. DICKS. Our committee has been concerned that we made a mistake with the 2-finger system versus using 10 fingers, and it is 10 fingers. Now, I understand, obviously, that does cause a cultural concern. I mean, I think we have to recognize that other countries may not think that is—they feel that they are being treated like criminals. And so it does present a problem. So maybe the facial digital picture is something that was done through ICAO, which is our UN, United Nations, group of experts on travel. This may not be a bad outcome.

The only other thing I would say is, I do not see anything wrong with having a person to have to put down where they are going to be. I think one of the questions we have had over the years is that people got into the country and we had no idea where they were. At least you have some place to start, and assuming that some people put legitimate information and I think most people would about where they are going to stay or what hotel they are going to be at, et cetera. I mean, it cannot be verified, but at least it is a start of collecting information about where these people are in the country. We need to get them out of here or find them. At least we have some place to start. So I feel that that ought to be considered.

Again, I am having a real hard time understanding why we ever got ourselves into a system that allows a person to get on the airplane, fly to Maine for eight hours and then take them off the airplane. To me, that just does not make any sense. I am to glad to hear you are trying to go in a different direction, but why did we do this in the first place? I mean, it is so ridiculous on the face of it, I cannot understand why we ever got ourselves into this.

Ms. DEZENSKI. We are living in the post–9/11 environment, and the parameters under which we operate are aviation systems, the parameters that we use to collect data, to accept risk and deal with that risk is much different than it was pre–9/11. And so I think what we are seeing here is the use of legacy systems and legacy approaches that now have to be updated based on how we want to manage our system, how we want to deal with our threats and vulnerabilities now.

And it is not uncommon that we run into scenarios like this where we may have access to some data but not all data. We may get some data at the time we need it but maybe not all of it. And so as we go through the systematic review process and we respond to mandates like we have in the Intelligence Reform Act, for example, to get the safest data sooner in the process. We are going to make those course corrections, but I think we would fully agree with you that the old way of doing things and getting that data late in the game is not where we want to be to identify those threats and deal with those threats as quickly as possible.

Mr. DICKS. Why didn't we set it up so you could check before the flight leaves rather than 15 minutes after it leaves? I mean, that is not that much of a time difference. Why was it done that way?

Ms. DEZENSKI. I cannot speak to—

Mr. DICKS. Isn't there a way it can be done technically? Is that what you were saying?

Ms. DEZENSKI. Well, there are most certainly technical limitations to when we can get all the data. I think it is mostly a reflection, though, of the fact that in previous times perhaps the threat and vulnerabilities did not necessitate that that information be received any sooner in the process. And now we know that is not the case. We need to get it sooner, we need to deal with those issues.

Mr. DICKS. Did you say this would be resolved?

Ms. DEZENSKI. We are trying to get the rule out as quickly as we can. Now, it will go through a notice and comment period.

Mr. DICKS. It does have a great record of keeping its commitments on reports or getting information back or doing things in a certain timeframe. How solid is this 2 months?

Ms. DEZENSKI. Well, we are doing the best we can to get this one out. Again, I think I have alluded to a lot of the concerns that we have been dealing with in trying to come up with a timeframe that is reasonable and does not have a negative impact on the operations for air carriers. We have a lot of things to consider in this process, and the last thing we want to do is put a requirement out there that leads to an effect that is worst than what we started with. So we really need to do this right.

Mr. DICKS. I can understand there might be a few last minute changes of people getting on this airplane that would then necessitate doing a check after the plane left. But there has got to be at least 95 percent of the people on that plane we know are going to be on that plane well before the plane takes off. So why couldn't they check it before it takes off, and then if they have to update it, update it. But at least do a check before the plane takes off.

Ms. DEZENSKI. You are absolutely right, some of that data is available. Some people come to the airport three hours in advance of their international flight. That data is available. We could start to do those checks. But it is not the case for every passenger that we are dealing with, so we have got to figure out what is the shortest window in which we can operate where we can get the vast majority of that data and perform our check and be able to get back to the air carrier with that board or no-board decision for that list of passengers. And of course this happens thousands and thousands of times, every time a flight takes off. So there are a tremendous number of operational issues and technical issues to take a look at on implementation of this requirement.

Mr. LUNGREN. The gentleman from Washington's time has expired. I just might say that I am constantly refreshed by the enthusiasm and intensity of your feelings on this, and I appreciate it. Now I know why you went to the Rose Bowl.

Gentleman, Mr. Pearce, is recognized.

Mr. PEARCE. Thank you, Mr. Chairman.

There seems to be questions whether or not fingerprints should be involved in a biometric passport. Briefly, do you all have an opinion?

Mr. MOSS. I think you have to recognize that any requirement that we would attempt to impose on other governments would then expect us to meet the same requirement. I think it is fair to say the administration has no position on the issue of fingerprinting American citizens as part of the passport process.

Ms. DEZENSKI. I can tell you that we are looking very closely at the enrollment process for US–VISIT and our biometric standards across the board to determine whether we want to move, for example, from a 2-print enrollment process to a 10-print enrollment process. There is a lot of discussion about how to get to the best use of fingerprints. We would certainly defer to the State Department on any thoughts with regard to using fingerprints, catching fingerprints as part of the U.S. passport issuance process.

I can tell you that some European countries are looking at adopting fingerprints, although I do not believe that any final decisions have been made, and they are looking at the use of those fingerprints within the E.U., not, for example, information that we could access.

Mr. PEARCE. Thank you. I think I am the only member in the committee with a border along the Mexican border, so I am very familiar with the WHTI and how it is supposed to aid in security along the border. I am also concerned that many residents in our district need to travel back and forth frequently, and so we worry about having a friendly border at the same time having a secure border, and that is a difficult balance.

As far as the efforts to implement WHTI, what efforts to date have been made to implement the processes of that, and is it going to be implemented by December 2007?

Mr. MOSS. Thank you very much for the question. The first point I would bring up is that we have still not published the Advance Notice of Proposed Rulemaking. It is very close to that publication. It should happen in the next, I would say, couple of weeks.

Elaine and I have traveled thousands of miles, literally, doing outreach. In fact, I was just last week in Arizona doing the same thing. We are trying to educate people, we are trying to make people understand that there is more than one phase to this program, that it does not all go into effect at one point.

Both State and the Department of Homeland Security recognize that different travel documents work better for different uses. For example, if someone is getting on an airplane or getting on a cruise ship and going abroad, that really is travel for which almost exclusively the passport is the appropriate document. We all recognize that the land border is a huge challenge.

In this regard, during the month of July, the State Department is contracting to have surveys done at 16 border crossing areas to help us get our handle on perhaps our key unknown piece of—

Mr. PEARCE. Will it be ready to go by 2007?

Mr. MOSS. That is what the law says, sir. [We are—]

Mr. PEARCE. Are the RT cards going to be allowed to be one of the documents used?

Ms. DEZENSKI. We are looking again at the RT concept. We have a couple of frequent traveler type programs that are in existence, which we have referenced as part of our outreach on this. We are going to move toward global enrollment in uniform Registered Traveler type programs to facilitate at the land borders—

Mr. PEARCE. Are we going to have the program kickoff to make sure that we can sustain it?

Ms. DEZENSKI. Absolutely.

Mr. PEARCE. Mr. Moss, what efforts is the State Department making to ensure that if we want to require passports to cross, that you can actually keep up with the load in a timely fashion? Again, these are my constituents who are going to be calling me asking me to call you, and I would like your home phone number as well if you have it.

[Laughter.]

Mr. MOSS. I will provide it, sir. The reality is that we are making major investments in cooperation with the Congress, and we will be talking to you about certain aspects of that, because we do need to increase capacity. Right now, this year, we are already issuing 10 million passports a year, some of them are probably to WHTI-related travelers. But as we look out a couple of years, we think that number could get up into the range of 15 to 17 million a year.

That is a big challenge for us, we have lots of initiatives underway, but we are going to need help from Congress as well.

Mr. PEARCE. Thank you, Mr. Chairman.

Mr. LUNGREN. The gentleman, Mr. Langevin, is recognized for 5 minutes.

Mr. LANGEVIN. Thank you, Chairman.

I want to thank you both for being here testifying today.

I wanted to turn my attention back to the durability lifespan of the biometric chip. I know the company that you are working with has assured us that it will last for the 10 years that it is expected to, according to what you just testified to, but one of the problems that I see is with a passport that has been somehow physically damaged, you can obviously see it, but if a chip has been damaged or we have all been in the situation where you are too close a magnetic source and the data on your credit card gets wiped off. And that is not going to be very obvious until the traveler gets to the airport.

So what are you going to do in that case when a traveler gets to the airport and his or her passport is damaged, the data is gone off the chip and they are about to get on a plane?

The second thing is if I am a potential terrorist and I know that they are going to look the other way or when I get to the airport they are going to let me on the plane, then they are going to do something to physically damage, intentionally damage the passport and the data chip and hopefully try to get on the plane without proper biometric screening. So can you address those questions for me?

Mr. MOSS. Certainly. I think the first point I would like to reassure you and others is that if the chip is damaged, as we say in our own rulemaking we will replace a passport with a damaged chip at no cost to the bearer. But the other point is, just as is the case right now, at the end of the day the default, if you will, security mechanism in the chip is actually the data page itself. As long as the data page is intact, you as a legitimate traveler will be able to board that aircraft.

You may, I would add, be subjected to some additional scrutiny, either entering the United States or entering another country without an operational chip, but I think you will be able to travel. [You will be able to travel, there is no "think" about it.]

I think on the point of deliberately damaging the chip and things of this nature, it is another issue. Clearly, I think part of the answer to that is data share. I talked a little bit about that before, about trying to identify [mollified] terrorist travelers before they travel.

I also think it is important to note in that regard that in some cases the only biometric we ever have on a truly dangerous traveler is in fact a photograph that has been acquired in some cases, getting back again to the value of a photograph.

Damaged chip, admittedly, they could do that, but we think that the chip is going to be very durable unless it really is deliberately attacked, and that will probably leave some evidence which would make an inspector or an airline official somewhat suspicious about the traveler.

Mr. LANGEVIN. Now, on that point, with respect to a chip potentially being damaged or if technology changes so quickly, have you thought about the issue of reducing the timeframe from 10 years down to 5 years, both to allow us to incorporate new technology or to ensure that the information is current or the chip is not damaged?

And within that, have you also factored in, even if you leave it over 10 years, you factored in data migration issues? As a former Secretary of State, we were always grappling with the issue of the new machines being able to read the old technology, and that is something that I would like you to address?

And can the State Department handle the additional production costs and associated activities that would go into reducing that timeframe?

Mr. MOSS. [Okay.] Let me see if I can deal, first of all, with the validity period, because I think that deals with two or three of the other issues. We have looked at the validity period issue, sir, and if we were to take our projected demand of 12, 15 million passports a year and go from a 10-year book to a 5-year book, it would not exactly double but it would probably go up by about two-thirds.

So now we would be back here with Congress looking for resources to build a passport system that could sustain 25 million passport adjudications or replacements a year. That would be a daunting challenge, I think. It certainly would be for State. [I think DHS would agree with me, the same way.]

In terms of technology, what we have tried to do is two things. One is, as I said in my earlier testimony, we have considerable unused capacity on the chip, so we are trying to, in one case, futureproof the technology so that if we decide, for example, to go with iris scans as a second biometric, additional photographs, finger scans, something of this nature, we do not have to change our technology.

The third point is, as technology evolves, one of our baseline objectives will be that it is always backwardly compatible so that the DHS passport reader in 2012 will be able to read passports issued in 2012 as well as in 2006. That is why the State Department is paying a lot of very bright people in the private sector, at NIST and at the Government Printing Office to help ensure that we can do that.

Mr. LUNGREN. The gentleman's time has expired.

The gentlelady from Virgin Islands, Dr. Christensen, is recognized for 5 minutes.

Mrs. CHRISTENSEN. Thank you, Mr. Chairman.

I am sure you know we are heavily dependent on tourism for our economic livelihood. Because so many of our visitors come from the U.S. mainland, I am going to be extremely concerned. Just yesterday I answered one question to the press on that, and I want your assurance today that my constituents and myself will not have the requirement imposed on us as it has been posed on the other countries in the Western Hemisphere.

Mr. MOSS. I would certainly invite you to make that comment as part of our advance notice of proposed rulemaking process, but I can assure you on both the State Department and DHS' side, we both recognize your constituents are U.S. citizens and people trav-

eling to the Virgin Islands or Puerto Rico from the United States are also U.S. citizens. We have no concept whatsoever, no thought whatsoever of imposing essentially an internal passport requirement on travel between U.S. territories and the United States, the main ones, I should say.

Mrs. CHRISTENSEN. Music to my ears.

[Laughter.]

I am also concerned about the rest of the Caribbean as well and the impact of the initiative on my neighboring Caribbean islands. And in December of this year, the passport or other executive document, as you will determine, will be required for all travelers to or from the Caribbean, Bermuda, Central America and South America.

You have just extended the time on the Visa Waiver Program, and there is a lot of concern in the Caribbean. What is the possibility that you would extend the time on the Western Hemisphere another year as well?

Ms. DEZENSKI. As I think we mentioned earlier, the advance notice of proposed rulemaking on the Western Hemisphere Initiative is still in the process of being cleared by the Department, both State and DHS, and ultimately OMB. We have most certainly taken into consideration the concerns that have come up about travel to and from the Caribbean, and we do understand that there are potential implications. We have looked at a couple different ways to phase in these options.

One of the reasons why we are doing this as an advance notice of proposed rulemaking is precisely because of some of these concerns and that we need to consider them as early in the process as possible. So although we have not issued specifics on what the proposed implementation date may be, we are certainly looking at some flexible requirements.

Mrs. CHRISTENSEN. What is in place for the visa waiver countries to prevent someone from fraudulently obtaining a passport overseas in another country, who is not on a watch list or in our databases, and entering the U.S. under the assumed identity based on their biometrics?

Mr. MOSS. I think I actually have some rather good news for you in that regard. The countries that are in the Visa Waiver Program have to meet a variety of requirements, but one of the things we also look at is the integrity of their passport system. These are all very sophisticated countries. Quite honestly, many of them have database access, for example, national registries of births and deaths and things of this nature, which do not exist in the United States.

I am very confident in the integrity of the way the U.S. passport is adjudicated. I certainly share that feeling about the way passports are adjudicated in the other visa waiver program countries as well.

Mr. LUNGREN. Thank you. There has been a request to have a short second round before we go to the next panel.

Let me just ask this, and we may be beating this to death, but it is very important for us in terms of a homeland security perspective, to make sure that the person standing before us is the person he or she purports to be. And some of us got excited about the ter-

minology, "biometrics," but I share the chairman's concern that what we are really doing is looking at a picture. The picture may be embedded in the chip so that you can see it come up in a comparison, but that is recalls you all are doing. It is not any sort of software analysis of the face.

Fingerprints are ubiquitous, and I understand the E.U. is more than thinking about it, I understand the decision is made that they are going to put fingerprints in their passports. But is the problem that if they put fingerprints in their passport, we cannot read them technically or that we will not be granted permission to utilize that against any database that they have?

Ms. DEZENSKI. My understanding at this point is that they would only be considering the use of those fingerprints within the E.U. proper. So, for example, if they are stored on the biometric chip, we would not be able to access that information when we scan that passport at the U.S. port of entry.

Mr. LUNGREN. Does that mean we would not be able to read it or we would not be able to read it and then access their database for identification purposes?

Ms. DEZENSKI. Well, actually, both. We would not be able to read that information on the chip, and there would be no link back to an E.U. or a member country database for any type of check.

Mr. LUNGREN. I understand the concerns you are expressing. My thought is, and I do not know if it is shared by other members of the panel, but that we ought to be in the vanguard of creating identifiers which will really answer the question, who is it in front of me, to the greatest extent possible.

For the life of me, I do not see anything better than fingerprints. I share Mr. Dicks' thoughts that if we are going to do that, we ought to go to 10 prints rather than 2. We ought to be in advance of that and then work our way in the diplomatic circles to try and get others to understand why it is important for us to have access. It is in their interest, it is in our interest if we are in a worldwide battle against terrorism.

That is why I understand what you are saying. I am not trying to harp on you, but my feeling is we ought to be in the vanguard, we ought be presenting it, we ought to be making the case for why this is the way to make sense. As the chairman has said many times, we are looking for needles in a haystack, and right now we are looking at the largest haystack possible, whether it has gone through passports or whether it is forcing people to go through checks.

And I have always thought, in terms of law enforcement and everything else that the idea is to limit the scope of the suspects that you are looking for. And to the extent we do not do that or give ourselves the tools to do that, we are making it more difficult for ourselves and we are making it far more expensive for ourselves.

So just sort of an expression of frustration that I have.

The gentlelady from California, if she has any more questions.

Ms. SANCHEZ. I would agree with the chairman. I am just amazed that we would require another country to put a chip in their passports and then when they come to our country we do not really use that. I mean, why are we putting those requirements on them if we are really not going to have any access to it?

Ms. Dezenski, I want to go back to the last question you did not get to answer. Could you answer that question for me, how many places currently issue NEXUS cards, how many issue FAST cards, how many issue SENTRI cards? And how many places do you believe your Department is going to plan to issue Registered Traveler cards?

SUPPLEMENTAL MATERIAL FOR THE RECORD

Question: Could you answer that question for me, how many places currently issue NEXUS cards, how many issue FAST cards, how many issue SENTRI cards? And how many places do you believe your Department is going to plan to issue Registered Traveler cards? (Page 68, line 1613)

Answer: Cards for NEXAS, FAST and SENTRI are issued by CBP at local (port of entry) enrollment center. The Current totals for each are as follows:

NEXUS—5 (Plus NEXUS Air Pilot)

Enrollment Centers	*Crossings*
Blaine, WA	Peace Arch
	Pacific Highway
	Point Roberts
Buffalo, NY	Peace Bridge
	Rainbow Bridge
	Whirlpool Bridge (NEXUS-only)
Detroit, MI	Ambassador Bridge
	Windsor/Detroit Tunnel
Port Huron, MI	Blue Water Bridge
Champlain, NY	Champlain
	Highgate Springs (VT)

NEXUS Air Pilot is operational at Vancouver International Airport, BC.

FAST—17

Southwest Border Locations:	*Northern Border Locations:.*
Brownsville, TX	Belleville, New Brunswick (Houlton ME)
Calexico, CA	South Derby Line, Vermont
El Paso, TX	Champlain, NY
Laredo, TX	Fort Erie, Ontario (Buffalo, New York)
Otay Mesa, CA	Windsor, Ontario (Detroit, Michigan)
Pharr, TX	Port Huron, MI
Nogales, AZ	Pembina, North Dakota
	Portal, North Dakota
	Sweetgrass, Montana
	Blaine, WA

SENTRI—2

Enrollment Centers	*Crossings*
Ca—Otay Mesa	Otay Mesa
	San Ysidro
TX—El Paso—Ysletta Port of Entry	El Paso—Stanton Street Bridge

With regard to the Registered Travel (RT) program, TSA's RT pilot tests are operating at five airports across the country: Minneapolis St. Paul (MSP); Los Angeles Internation (LAX); Houston George Bush Intercontinental (IAH); Boston Logan (BOS); and Reagon National (DCA). A new pilot at Orlando has been launched to assess the feasiblity and effectiveness of using a public/private sector business model to implement RT.

Ms. DEZENSKI. I do not have the specific numbers with me, but I can certainly follow up for the record to get those enrollment sites for you.

I can tell you that it is fairly limited. I think it is important to keep in mind that NEXUS and FAST and SENTRI were never envisioned as alternatives to passports. We think they are tools that can be useful in meeting Western Hemisphere requirements, but the way that the enrollment process is set up for these types of programs, it is normally at our busiest crossings and caters to those folks who cross very frequently. So we, again, have focused on those ports of entry where we have the highest volume.

Now, we are expanding all of those programs over the next couple years, but I think it is important to get back to this idea of the Registered Traveler concept, because we need to look more broadly at how to encompass into some type of global process that would facilitate some type of card, particularly at the land borders.

As far as the RT Program goes, we are in of course the pilot phase. We have agreed to extend that pilot I believe through September, and then we will make some determinations at the Department level about how we continue that program.

So decisions about the number of enrollment centers, for example, will be linked into the broader discussion within the Department about where we want that program to go. So there is no specific decision on that right now.

Ms. SANCHEZ. And then, Mr. Moss, when I was younger I used to live in Italy and I had an American passport, and during my stay there, during one of the years my passport expired and I went down to the embassy and I redid it. Compared to what was issued here, it was pretty much hand-done, it seemed to me, at the embassy.

My question for you is two-pronged. When you lose your passport in a place like Italy and you go to the embassy, do you get a temporary passport to go back or do you get issued a new passport?

At that time, I had a new passport issued within 3 days, for example, which was a re-up of another 7 years or 10 years or whatever the time was at the time.

So under the two cases, if I lost it or if I was living in a different country and I needed to go and get it renewed, would I even get the same kind of passport that I had issued with the embedded chip and everything from an outpost like Rome, Italy, versus if I am in Uzbekistan or some other place?

A load of questions there, but I am trying to understand what do we really have in hand?

Mr. MOSS. Let me deal with the case of someone who is living in Italy or living in Uzbekistan and their passport is about to expire. They live there, they contact our embassy, they turn in their old passport, we do data entry, scan the photograph and that data then moves electronically back to one of our production facilities in the United States. They make the passport the same day, and it comes FedEx, as of July 5, back to the embassy abroad. In a place like Rome, Italy, you will usually have it within 3 or 4 days after you walk in the embassy.

In the case of someone who is traveling abroad and may be in Italy today and in Germany tomorrow, we will issue a 1-year tem-

porary passport. When you return to the United States after your trip, you turn that into us and you then get a full 10-year validity passport, paying for it only once.

We went to the decision, by the way, of repatriating the production back to the United States because it gave us the security system. We make the same passport that is available in Rome as is available in New York or Washington. More importantly, it was also a good use of money.

Placing this highly sophisticated passport production and personalization equipment overseas [just] simply is not a good use of the taxpayers' money.

Ms. SANCHEZ. What is the difficulty having 120 different countries that—

Mr. MOSS. Actually, I think you can get a passport at I think it is 240 different posts around the world.

Ms. SANCHEZ. There are only 120—okay. Thank you.

Mr. LUNGREN. The chairman of the full committee, Mr. Cox, is recognized for 5 minutes.

Mr. COX. Thank you, Mr. Chairman.

I want to begin by again thanking our witnesses. You are working on some very important matters here.

I also want to see if I can peel down a little bit further on this question of where we are going, why and what is the purpose of all of this. I hope that our purpose is data security to the extent that we are imposing new requirements on travelers, our allies and other countries around the world, and that it is not an exercise, it is not something for its own sake. So I think it is a fair question to always ask, 'what is the security payback"?

My judgment is that there is little to no security payback in the so-called biometrics that is the subject of the Department's recent decision, and that is why I think it is fine to put if off. Because, quite honestly, when it is all in place, there is still no real additional security or at least it is of marginal value.

I do agree, for example, that looking at a bigger picture on the screen instead of looking at a little picture is a marginal improvement. It has been commented on several times during this hearing that we are still just looking at a picture. That is all we are doing.

I am struck that the mandatory biometric of facial recognition is essentially useless in finding known terrorists because there is no existing database. The same is true for iris scans or all the other fancy things that we might, as Americans, subject ourselves to.

As Chairman Lungren was pointing out, there are international databases of criminals' fingerprints that someday we might reach some international understanding to share a little bit more broadly.

I have to say that putting the chip on the card, linking the chip to the photo, with all of its shortcomings, sent me down a path that I am even less comfortable with than the fingerprints. I do not know what is going to go on the chip. It is a rather elaborate undertaking to avoid doing the obvious, which is checking a real biometric, such as a fingerprint, for a passenger, a traveler through the airport just by touching something.

But to be very explicit about it, my privacy interest in the distance between the ridges on my fingertips compared to my privacy

interest in my tax records, my credit card usage, the library books I read, my medical history, my employment history and so on, all of which I think we would all agree in this room ought not to find its way into the chip on this card, is negligible.

I do not want the government to know what I am reading, I do not want the government to know anymore than it needs to know about my medical history or all the other things that make me Chris Cox. I do think that something that establishes that I am Chris Cox and not Tom or somebody else around here so that I can go through the airport and proceed on my way is a help to me.

So the point that we are trying to establish here is what is it going to take to find these terrorists? And if the iris scan that I have subjected myself to as a participant in the Registered Traveler Program is not going to produce a database that has terrorists in it, it is of relatively less value. I do think the chairman's right that we can reduce the size of the haystack that way, so it is a voluntary program, the Registered Traveler is, and maybe that is fine.

But for most people who may not want to participate in such a voluntary program, the question is, how are we going to not focus on them in the most efficient, cheap, fastest way if they are not terrorists? And it seems to me that that question is put very neatly by your predecessor who is going to testify on the next panel, Stewart Verdery, and I just want to quote from his testimony and ask you to react.

He says, "I recommend that the United States match the bold steps of the European Union to include fingerprints in passports. The U.S. should advocate for fingerprints as a mandatory biometric in passports at ICAO," and of course that underscores the fact that that is not the U.S. position.

And, Mr. Moss, you said there is no administration position on this one way or the other, I believe, a moment ago. So we are not leaving it in ICAO, we are just simply saying that they have adopted fingerprints as a secondary way to do this after facial recognition, and we are just going along with the flow.

Quoting from Mr. Verdery, "At a time when we are going to great lengths to build antiterrorism and law enforcement systems based on fingerprints, we will never be able to fully engage other countries if we decline, ourselves, to do what is needed."

So I would just ask for your reaction to that?

Ms. DEZENSKI. I think my former colleague makes some good points. I want to go back to something Frank Moss said a while ago, which is we are at the beginning stages of using biometrics. We are really just starting, and I think we are going to see the evolution of the use of biometrics, we are going to see more interoperability between databases, we are going to see more cooperation on the international front.

But we have got to start somewhere, and I think if I want to leave you with one message it is not to think that we are somehow not utilizing fingerprints. It seems to be the focus of where you want to go, and the use of fingerprints starts very early in the process.

If you need to obtain a visa, if you are outside of the Visa Waiver Program countries, when you apply to the U.S. consulate, you are required to give 10 fingerprints. It is used to run a check against

what is called IDENT and IAFIS, which contains extracts of criminal records and what not. So that process happened when we are issued a visa.

If you are in a Visa Waiver Program country, not only do you have the biometric requirements that we talked about in the past, but you are also enrolling on your first time entering the U.S. End of the program using your fingerprints. Right now it is two. We may at some future time look to expand to a 10-print, but those fingerprints are captured and when you come back for your subsequent visits you are checked against that fingerprint database.

Again, we are at the beginning stages but there are multiple layers in this process that utilize biometrics in different types of ways. And there are two issues: One is verifying you are who you say you are, and the second piece is being able to run a test to ensure that you are clean. So we use biometrics to achieve both of those objectives.

Mr. COX. I am glad that that is where we were headed. I think it is manifest that we are not there now, and I hope we will increasingly see our way clear to doing these things.

Mr. LUNGREN. The gentleman from Washington, Mr. Dicks?

Mr. DICKS. I want to make sure I got this straight. You said that for visa waiver countries, countries that are in the Visa Waiver Program, you check two fingerprints, right? Why can't you, if the person who has got the passport, can that same person check the—if this person says he is this person and he is from a Visa Waiver Program, can he check the fingerprints at the same time?

Ms. DEZENSKI. Can the inspector check the fingerprints?

Mr. DICKS. Yes.

Ms. DEZENSKI. Yes. Let me walk you through the process of someone traveling from a VWP country, enters the U.S., and let's assume that they have e-passport, so it has the digital photo and the biometric chip. When that person enters at the U.S. port of entry, their passport would be scanned in and read by our reader.

It would look at the biographic data and would compare that to what is in the passport, and this chip would be unlocked, if you will, to display the picture that is encoded, which should match with the person standing in front of them and with the digital photo embedded in the actual passport.

The second part of this process is the use of fingerprints for that VWP traveler. If it is their first time into the country under the US–VISIT requirement, we do an enrollment process which checks their fingerprint against numerous databases and ensures that they do not have some terrorist link. And as they come in for subsequent visits, they are again asked for their fingerprint. We also take a photo, by the way, but they are asked for their fingerprint, and we do another check to make sure that the fingerprint in fact matches the record that we have on file for that person. So it is a two-part process.

Mr. DICKS. And that is done right there when the person comes through.

Ms. DEZENSKI. At primary.

Mr. DICKS. But it is not part of the passport. You have to go into the U.S.?

Ms. DEZENSKI. The fingerprint is not encoded on the passport.

Mr. DICKS. Right. We know that.

Ms. DEZENSKI. Right. That is right.

Mr. DICKS. But you have to use the US–VISIT system in order to use it.

Ms. DEZENSKI. That is right, but it is all integrated into the reader.

Mr. DICKS. On non-visa waiver countries, you use 10 fingerprints. Now, in the testimony it says if you get into the question of quality of fingerprints, you are much better off to have 10. Why did we not do 10? I know there was a big rush to get something deployed, but the 10 is so much more effective. And if we did it for the non–Visa Waiver Program countries, why didn't we do it for visa waiver countries?

Ms. DEZENSKI. There are a couple of reasons. One, of course, is the facilitation piece. When you apply for a visa, there is more time in the process. You can take 10 prints, you could run that check if it takes 20 minutes or 30 minutes, usually you are still in the consular office.

Mr. DICKS. That is whether it is a visa country or a non-visa country, right?

Ms. DEZENSKI. Well, you are only applying for a visa if you are outside of the VWP. So this would affect travelers coming from—right. So that is a different scenario than when you are at the port of entry standing in line along with thousands of other people, and we need to facilitate you through US–VISIT. There is no doubt, a 2-print process is much quicker, but I will tell you that there has been a lot of discussion about whether we move to a 10-print enrollment versus a 2-print. The initial decision was made to use a two-print process. We will be looking at that as we move forward to determine whether or not we need to revise that policy.

Mr. MOSS. Mr. Dicks, I would just like to clarify just so that we do not leave you with a misunderstanding. At this point, though, even in the visa waiver traveler situation, we are still only collecting two fingerprints from the traveler at this time. Our goal over the next couple of years, as not only State and DHS ramp up, but so do the agencies that have to read these prints ramp up their capacity, is to migrate towards 10. But right now, if you are applying, as someone asked me in Saudi Arabia, we are taking your two index fingers at this point in time.

Ms. DEZENSKI. I stand corrected.

Mr. DICKS. Well, okay. That is important to know because you would wonder why if you are doing 10 there, why wouldn't you do 10 in the other situation? That is the only question I had.

Thank you, Mr. Chairman.

Mr. LUNGREN. Before we let you go, let me just ask one last question here. You say in this program not only do you have your embedded passport and you run it through the scanner or reader once we have the readers in place, but then a separate action is to capture the two fingerprints. And on the first occasion the person comes in you run those fingerprints against our watch list database, correct? But, obviously, we are not running them against any European database.

Ms. DEZENSKI. We are not, but we do receive information from INTERPOL, for example, that is routinely put into our system and

used for those types of checks. So although we do not have a real-time link to INTERPOL, we do get information from those sources and put that into our system.

Mr. LUNGREN. So even if the E.U. passport had embedded in it fingerprints, we could not read that, so there would be no way for us to check the fingerprint of the person who is actually presenting themselves with the fingerprint that is embedded in the European passport at some time when they have that as captured.

Ms. DEZENSKI. We would only be able to read it if they allowed us to do so. So they would have to put the information on the chip and give us permission to read it.

Mr. LUNGREN. I understand. I understand. What you are saying is when we check it against our watch list, if they are not on our watch list, they get a pass on that. And then you are saying when they come back, we match their prints with the previous prints given so that we just make sure they are using the same alias they used before.

Ms. DEZENSKI. That is correct, but there is also a continual vetting process. So as we get new information—

Mr. LUNGREN. No, I understand that.

Ms. DEZENSKI. —we are checking our files.

Mr. LUNGREN. It just strikes me that in the law enforcement and in the criminal justice community, we know how many mistakes are made with facial identification. Eyewitness testimonies are often times thrown out or are wrong and so forth. I know we are going to have trained people looking at it and they have got the one picture and the other picture. But you have got someone with fingerprints, you have got them dead to right. That is why I am just saying our whole experience has been that fingerprints are the way to go.

I appreciate it, and I just want to thank you for your testimony. It has been very, very helpful for us. We appreciate the work that you are doing.

Other members may have other questions they might submit in writing to you, and we would ask if you would respond to that in a timely fashion.

And we appreciate the work you are doing. Thanks.

Ms. DEZENSKI. Thank you.

Mr. LUNGREN. I now call the second panel.

I would tell the other members that are here, we are expecting a vote around 1 o'clock. We are supposed to have a 15-minute vote, followed by a 10-minute debate, followed by a 15-minute vote, followed by a 5-minute vote. It would be my thinking that when we have the first vote called, go back and vote then and then come back here because we have about a 30-minute period of time if you look at the two 15-minute votes and the 10-minute debate, and resume.

I appreciate the indulgence of the second panel, having sat through the first bit of testimony. As I explained, we will have a vote momentarily. My expectation is that we will go over there and vote, come back for perhaps a half hour, then go back for the last two votes and then return.

I recognize at this time Dr. Martin Herman, the information access division chief for the National Institute of Standards and Technology, to testify.

And, again, I would just mention that your full written testimony will be placed in the record in its entirety, and we would ask you to try and limit your opening remarks to 5 minutes. Thank you.

STATEMENT OF DR. MARTIN HERMAN, INFORMATION ACCESS DIVISION CHIEF, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Mr. HERMAN. Thank you, Chairman Lungren, Ranking Member Sanchez and members of the subcommittee. And thank you for the opportunity to testify today about the biometric activities at the National Institute of Standards and Technology, which will help secure Americas' borders.

Under the USA Patriot Act and the Enhanced Border Security and Visa Entry Reform Act, the Attorney General and the Secretary of State, through NIST, were directed to make recommendations for means of verifying the identity of travelers entering the United States with visas.

These recommendations were made in a joint report to Congress dated February 2003. Since this report was issued, NIST has continued to conduct an extensive biometric research and evaluation program.

NIST, in close collaboration with the Department of Homeland Security, Justice, Defense and State, has performed many tests of fingerprint and face recognition systems in support of its statutory mandates. Fingerprint tests have been performed at NIST on the FBI's Integrated Automated Fingerprint Identification System, or IAFIS, on DHS' IDENT system, which is of course part of the US–VISIT system, and we have also done tests on many commercial vendor systems.

In the face recognition area, we have done tests on many commercial as well academic systems.

To support these tests, NIST has acquired very large sets of data, including 128 million fingerprint images taken from 18 million subjects by several federal, state and county agencies.

NIST Patriot Act recommendations are as follows: For one-to-one verification matching, NIST recommends the use of one face image and two index fingerprints, and all three biometrics should be stored in image form.

For one-to-many identification matching, NIST recommends the use of 10-slap fingerprint images, and these 10 would be used for enrollment and checking of large databases.

For both recommendations, the fingerprint images should conform to the ANSI/NIST 2000 standard. This standard, is also used in law enforcement for the electronic exchange of fingerprint images and is used to exchange fingerprints between the FBI and INTERPOL as well as with FBI and United Kingdom's home office.

Face images are not recommended by NIST for large-scale identification applications if fingerprints can be used.

For verification matching, NIST tests have shown that contemporary fingerprint systems are substantially more accurate than face recognition systems in operational environments. However,

this should be qualified by the fact that any advances in face recognition technology since the last NIST face test, which occurred in the year 2002, any advances in technology have yet to be evaluated. And we do believe there have been improvements in face recognition since then.

The two fingerprint accuracy for the US–VISIT two fingerprint matching system is 99.6 percent with a one in 1,000 false positive rate. This means that one in 1,000 imposters will falsely be permitted to pass the checkpoint. The best 2002 face recognition accuracy using a single-face image with controlled illumination was only 90 percent when one in 100 imposters are allowed through.

When outdoor illumination, which of course is totally uncontrolled, was used in 2002, the best accuracy was 54 percent.

Currently, in the US–VISIT system, illumination is uncontrolled when face images are obtained using the US–VISIT cameras. Clearly, for the current US–VISIT implementation, two fingerprints are a much better solution than a single uncontrolled face image.

For identification matching, expensive testing by NIST of commercial fingerprint systems has confirmed the requirement of 10-slap fingerprints. For all systems tested, the accuracy increases as the number of fingers increase. So the accuracy of searches using four or more fingers was higher than the accuracy of two finger searches, which is higher than the accuracy of single finger searches.

For the US–VISIT fingerprint matching system, the overall accuracy using index finger pairs is 96 percent. For low-quality fingerprint data, the accuracy falls to 53.6 percent, while for high-quality data, the accuracy is 99.6 percent.

The only tested method for improving matching accuracy for databases with lower image quality, or lower fingerprint quality, is to increase the number of fingers used. When 10 fingers are used, the accuracy for the most accurate commercial system tested exceeded 99.95 percent.

Iris recognition is a potentially valuable technology that needs considerably more testing to determine its accuracy in operational environments. NIST is planning an iris data collection effort using 10,000 individuals over the next year and will perform iris tests over the next 2 years.

Thanks for the opportunity to testify, and I would be happy to answer any questions.

[The statement of Mr. Herman follows:]

PREPARED STATEMENT OF DR. MARTIN HERMAN

Chairman Lungren, Ranking Member Sanchez, and members of the Subcommittee, thank you for the opportunity to testify today about the biometric activities of the National Institute of Standards and Technology (NIST) that will help secure America's boarders.

Under the USA Patriot Act (Public Law 107–56) and the Enhanced Border Security and Visa Entry Reform Act (Public Law 107–173), the Attorney General, and the Secretary of State, in consultation with NIST were directed to make recommendations for means of verifying the identity of travelers entering the United States with visas. These recommendations were made in the joint report to Congress entitled "Use of Technology Standards and Interoperable Databases with Machine-Readable, Tamper-Resistant Travel Documents," dated February 2003.

Since this report was issued NIST has continued to conduct an extensive biometric research and evaluation program. In particular, NIST is studying three types of biometric technologies: fingerprints, facial recognition, and iris recognition. These three biometrics were specified for international travel documents by the International Civil Aviation Organization (ICAO). ICAO has specified face biometrics as required for such documents, while fingerprints and iris are optional.

NIST, in close collaboration with the Departments of Homeland Security, Justice, Defense, and State has performed many tests of fingerprint and face recognition systems to support its statutory mandates. Fingerprint tests have been performed on the FBI's Integrated Automated Fingerprint Identification System (IAFIS), used to perform criminal background checks; DHS's Automated Biometric Identification System (IDENT), used as part of the US–VISIT system; and many commercial vendor systems. Face recognition tests have been performed on many commercial and academic systems.

To support these tests, NIST has acquired very large sets of data. For example, NIST has obtained 128 million fingerprint images taken from 18 million subjects by several Federal, State and County agencies. This data includes rolled, slap, and flat fingerprints captured either from paper using ink or from live-scan readers. A rolled fingerprint involves capturing the full finger image as it is rolled from one edge of the fingernail to the other. Slap fingerprints involve capturing the four fingers of a hand placed together on a flat surface, followed by a separate capture of the thumb. A flat fingerprint captures the image of only a single finger placed on the surface.

NIST has performed tests of both verification matching and identification. Verification is a one-to-one comparison in which the biometric system attempts to confirm an individual's claimed identity. The individual's biometric information is submitted and compared to an existing template. In US–VISIT, this occurs during the time of border crossing when the system determines whether the person holding the travel document is the same person to whom the document was issued.

Identification is a one-to-many comparison where the biometric system attempts to determine the identity of an individual. An individual's biometric information is collected and compared to all the templates in a database. In US–VISIT, this occurs during the time of enrollment when a person is checked against a watchlist derived in part from the FBI criminal database as well as the IDENT databases. First a database is checked to determine whether the person is on the watchlist. Second a database is checked to ensure that the person has not been previously enrolled in the database under a different name.

NIST's activities require substantial financial and logistical support from external agencies, whom we are fortunate to collaborate with. For example, research and evaluation activities are coordinated through the National Science & Technology Council's Subcommittee on Biometrics. NIST has also been actively working with several standards development organizations in development of fingerprint, face, and iris standards. These organizations include the International Organization for Standardization (ISO), the International Committee for Information Technology Standards (INCITS), and the American National Standards Institute (ANSI).

PATRIOT ACT RECOMMENDATIONS

For one-to-one verification matching, NIST's Patriot Act recommendation is to use one face image and two index finger prints. All three biometrics should be stored in image form. The face image should conform to the ANSI/INCITS 385–2004 standard. The fingerprint images should conform to the ANSI/NIST–ITL 1–2000 standard with 500 dots per inch (dpi) scan resolution.

For one-to-many identification matching, NIST recommends the use of ten slap fingerprint images stored in type 14 ANSI/NIST–ITL 1–2000 formatted records. These 10 fingerprints could be used for enrollment and checking of large databases. This ANSI/NIST standard, entitled "Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information," is also used for the electronic exchange of fingerprint images, and is currently used for law enforcement purposes to exchange fingerprints between the FBI and Interpol as well as with the United Kingdom's Home Office.

Face images are not recommended by NIST for large scale applications.

It is important to note that NIST's process for arriving at these recommendations and therefore the recommendations themselves, do not take into account likely impacts of implementing these recommendations on the U.S. economy, international reaction or contemplate the resources necessary to implement.

Again these recommendations were issued in a joint report to Congress. Since this report was issued, NIST has conducted extensive testing of biometric systems that continue to support these recommendations.

VERIFICATION

To verify a person's identity, NIST tests have shown that contemporary fingerprint systems are more accurate than face recognition systems in operational environments. However, this should be qualified by the fact that NIST has not tested facial recognition since the 2002 Face Recognition Vendor Test (FRVT). We believe there have been improvements in facial recognition since then. Department of State, for example, reports having success with facial recognition, both in one-to-one and one-to-many verification, with its Diversity Visa Program and in certain non-immigrant visa applications. Also the Face Recognition Grand Challenge, a development effort funded by multiple federal agencies and managed by NIST, aims to reduce the error rate by and order of magnitude over these levels. Preliminary results show that the community has met this goal in laboratory environments, but a definitive answer will not be available until completion of FRVT 2005.

Based on what we found in 2002, the two-fingerprint probability of verification (or true accept rate, TAR) for the US–VISIT two-fingerprint matching system is 99.6 while the best 2002 face recognition probability of verification was 90 percent using a single face image with controlled illumination. (Controlled illumination involves controlled light sources that illuminate the face while taking the picture). Additional FRVT 2002 results show that face recognition performance decreases significantly under uncontrolled conditions; the best probability of verification was 54 percent when using outdoor illumination. Currently in the US–VISIT system, illumination is uncontrolled when face images are obtained. Based on the 2002 data, even under controlled illumination, the error rate of face recognition is 25 times higher than the two-fingerprint results. Clearly, for the current US–Visit implementation, two fingerprints are much better solution than a single uncontrolled face image.

IDENTIFICATION

For identification applications, extensive testing by NIST of commercial fingerprint systems has confirmed the requirement for ten slap fingerprints. During the Fingerprint Vendor Technology Evaluation, 2003, again funded by multiple federal agencies and managed by NIST, eighteen different companies? products were tested, and thirty-four systems were evaluated. Different data subtests measured accuracy for various numbers and types of fingerprints, using operational fingerprint data from a variety of U.S. Government sources. 48,105 sets of fingerprints (393,370 distinct fingerprint images) from 25,309 individuals were used for analysis.

For all systems tested, the accuracy increases as the number of fingers increase. The improvement is both large and consistent. Although the actual benefits were found to vary by dataset and by system, the general trend was quite consistent. The accuracy of searches using four or more fingers was higher than the accuracy of two-finger searches, which was higher than the accuracy of single-finger searches.

These results are strongly dependent on fingerprint image quality. For the US–VISIT fingerprint matching system, using Department of State (DOS) Mexican visa Border Crossing Card (BCC) data, the probability of identification (or true accept rate, TAR) using index finger pairs is independent of background database size over the range from 100,000 entries to 6,000,000 entries. Using the operational thresholds, the probability of identification is 96 percent. If, however, fingerprint quality rather that database size is the controlling factor, then for low-quality data, the probability of identification falls to 53.6 percent. With high quality fingerprint images, the probability of identification is 99.6 percent. Image quality is important since the fingerprint quality of most archival law enforcement databases is lower than the quality of the data presently being collected by US–VISIT and will remain so for some time into the future. The only tested method for improving matching accuracy for databases with lower image quality is to increase the number of fingers used. When 10-fingers are used, the probability of identification for the most accurate commercial system tested exceeded 99.95 percent, with a false accept rate (FAR) of 0.01 percent.

Details for all the results described here can be obtained at *http://www.itl.nist.gov/iad/894.03/pact/pact.html.*

IRIS

Iris recognition is a potentially valuable technology that needs considerably more testing to determine its accuracy in operational environments. A recent non-NIST study of iris recognition has shown failure-to-enroll rates of about 2 percent. This means that 2 percent of the time, the system cannot perform an iris match. Fingerprints have close to zero failure-to-enroll rates. NIST is planning an iris data collection effort using 10,000 individuals over the next year to obtain a vendor-neutral data set in operational environments. This plus other large-scale data sets will then be used to perform iris recognition tests over the next two years.

CONCLUSION

As the Committee can see, NIST, in close partnership with federal sponsors and partners, has a vibrant biometrics program in the areas of fingerprint and facial recognition, and is also planning activities in the area of iris recognition. NIST tests have demonstrated that fingerprints are significantly more accurate than facial recognition for current US–VISIT applications, while iris recognition needs further assessment.

Thank you for the opportunity to testify. I would be happy to answer any questions the Committee might have.

Mr. LUNGREN. Thank you very much, Dr. Herman, for your testimony.

Now, the Chair would recognize Mr. Stewart Verdery, Jr., principal at Mehlman, Vogel and Castagnetti, to testify.

STATEMENT OF STEWART VERDERY, PRINCIPAL, MEHLMAN, VOGEL, AND CASTAGNETTI, INC.

Mr. VERDERY. Thank you, Mr. Chairman and Ranking Member Sanchez, members of the committee. Thank you for the opportunity to return to your committee to talk about how we should be using biometrically enhanced documents to secure our borders.

As you mentioned, I am at Mehlman, Vogel, Castagnetti. I am also Adjunct Fellow at the Center for Strategic and International Studies.

As was mentioned by Chairman Cox during the prior round, I was Assistant Secretary for Border and Transportation Policy the first few years of the Department, and I am excited to have the chance to be here, along with my former colleagues, Frank Moss and Elaine Dezenski. We had a great relationship with State, you can see all these programs are working together, and Elaine is doing a great job of following in our footsteps and moving the ball forward on a number of these key issues.

During my time at DHS, the Department deployed revolutionary uses of biometrics to secure our borders and transportation systems, and the most famous of these was US–VISIT and it seems it is now getting a lot of, I believe, misplaced criticism for not yet encompassing 100 percent entry-exit systems.

Secretary Ridge took the bold step of being willing to build a system in increments, because for many, many years before nobody could figure out how to do it all at once, essentially, and so nothing happened. And so he took the steps that we are going to airports and seaports, we are going to do exits, we are going to land borders in stages, in increments. And because of that decision, we now have 100 percent biometric review of all foreign visitors at air and seaports, of all visa holders at certain land ports of entry and of certain visitors departing the country at designated air and seaports.

And I might just mention the 9/11 Commission took a very hard look at US–VISIT and basically said that DHS was on the right track, just to do it faster and better.

The announcement last week by Secretary Chertoff concerning the Visa Waiver Program I believe was an appropriate one. As has been mentioned today, the original and worth goal of the Enhanced Border Security and Visa Entry Reform Act of 2002 was to bring biometrics to the border and to leverage ICAO to make that happen. The decision by ICAO to mandate a digital facial image, which could be compared to the person presenting the passport, could rep-

resent a marginal increase in security by detecting persons with forged or stolen passports.

However, as my colleague just mentioned, the software that would allow effective comparisons in actual field environments without generating unacceptable numbers of false positives is still under development. Allowing an additional year until October of next year to ensure interoperability of documents and document readers and enhancements to the facial recognition software is a wise one.

As Mr. Moss outlined, biometrics will soon play a key role in the security of passports issued to U.S. citizens. It is clear that a well-designed U.S. passport program is essential to securing our own borders to detect foreign imposters and perhaps even those entitled to a U.S. passport with ties to terrorism or serious criminal behavior.

It is more important to deploy an effective program, utilizing the best technology and procedures and privacy protections than to rush pilot projects out the door.

Moving forward, biometrics can provide significantly greater benefits to securing our borders and facilitating international travel, and my testimony goes into a number of these, I will mention a couple here briefly.

I do agree that DHS needs to go move to an 8-or 10-print solution as opposed to 2-print. This was in our original proposal that when it was announced that we would migrate to this because of the reasons mentioned of the overload of the IDENT and the possibility that some latent prints might not be picked up under the two-print system but no one should think that that means we should get rid of IDENT. The IAFIS system is incapable of operating as a real-time system, so the system has to built on 10 prints in IDENT, not IAFIS.

Second, as Chairman Cox mentioned, the United States has never advocated mandatory collection of fingerprint information in foreign passports, in part, because we have never required our own citizens to provide fingerprints in our passport applications. And the United States the larger world community then are essentially building out two elaborate but somewhat conflicting border management systems.

In one, governments are going to great lengths to collect fingerprints, to share those amongst their own agencies, to share them internationally through INTERPOL and other mechanisms. In the second system, we are building out elaborate systems of tamper-resistance passports and travel documents and readers of those documents capable of doing biometric comparisons. However, the mandatory biometric of facial recognition cannot be utilized to find a known terrorist or criminal from the database because there is no such database.

And I agree with the chairmen, both Chairman Lungren and Chairman Cox, and others, the historical resistance of government to fingerprint law-abiding citizens, not only in the U.S. but in Japan and Australia and other places, is weakening. The collective weight of 28 million successful enrollments in US–VISIT without privacy violations, without slowing down commerce, without horror stories is huge.

People are now becoming more willing to put aside nervousness about fingerprints aside to cut off the lifeblood of terrorists and that is mobility across borders. I recommend that the U.S. match the bold step of the European Union to include fingerprints in passports and that we should go back to ICAO and advocate it as a mandatory biometric.

Talk for just a second about how biometrics can help on the land border, an issue that came up earlier. It is absolutely critical that Congress aggressively fund US–VISIT, that land border implementation is not delayed. Travel documents have to be retrofitted or reissued to include information capable of being read wirelessly. Travel lanes have to be constructed or altered to allow that connectivity.

The exit feature is no less daunting. A reasonable goal over the next couple of years is construction of a system that would tell us when people have left, whether or not they have abided by the terms of their visa. The air side is also tricky. I think they are now ready to make decisions on how the air component is going to work with biometrics.

Recently, I had a great example in Texas of finding a sexual predator trying to get on a plane, went to check out, US–VISIT caught him, law enforcement officials got him before he got on the plane, and he is now in jail.

In my prepared testimony, I talk for a bit about what a guest worker program should look like, the use of biometrics to secure that. Just three quick recommendations: Any new applicant for a guest worker program should be required to submit 10 fingerprints for an IDENT/IAFIS review for terrorism and criminal activity; any new entrant should have a unique biometrically enhanced identification card that can serve as a travel document and an employer verification document. I will skip over the part about international registered traveler; absolutely critical to have that done.

The last thing I would mention, it is very important that DHS and the rest of the government, the State Department increase their engagement with the international community. That means bilateral negotiations on fingerprint sharing and other biometric and biographic information sharing to make those checkpoints useful. We only can do what we do, and sharing information is absolutely critical.

It is absolutely imperative to begin negotiations now with the European Union to make interoperability between US–VISIT and our bio-visa program, on one hand, and their visa information system that is being developed, on the other hand, interoperable. People are not going to accept the fact that they know something we do not and vise-versa, and we have to go back and work with them.

With that, I will be happy to answer any questions, and I thank you for the opportunity to be here today.

[The statement of Mr. Verdery follows:]

PREPARED STATEMENT OF C. STEWART VERDERY, JR.

INTRODUCTION

Chairman Lungren and Ranking Member Sanchez, I thank you for the opportunity to return to your committee to discuss the use of biometrically-enhanced documents to secure our country's borders. I am currently a principal at the consulting firm Mehlman Vogel Castagnetti, Inc. I also serve as an Adjunct Fellow at the Cen-

ter for Strategic and International Studies, although the views in this testimony are my own and do not represent CSIS which does not take policy positions.

As you know, following confirmation by the Senate in 2003, I served as Assistant Secretary for Border and Transportation Security Policy and Planning until my resignation from the Department of Homeland Security in March of this year. In this capacity, I was responsible for policy development within the Border and Transportation Security Directorate, reporting to Under Secretary Asa Hutchinson and Secretary Tom Ridge. BTS coordinated policy development and operational activities in the fields of immigration and visas, transportation security, law enforcement, and cargo security which largely were carried out in the field by BTS agencies—U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), and the Transportation Security Administration (TSA).

I am excited to have the opportunity to appear after the Committee has heard from the Department of State's Deputy Assistant Secretary for Passport Services Frank Moss and Acting Assistant Secretary for BTS Policy Elaine Dezenski. I am proud of the extremely productive relationship DHS formed with the State Department during my tenure and especially of the many initiatives I was privileged to pursue with Mr. Moss. And both as my former deputy and as my successor as Assistant Secretary, Ms. Dezenski has demonstrated great skill in tackling difficult public policy issues such as those being discussed today.

BACKGROUND

During my time at DHS, the Department deployed revolutionary uses of biometrics to better secure our borders and domestic transportation systems. Most famous of these success stories was the US–VISIT program. This initiative, discussed in full below, has come under criticism in recent months for not yet encompassing a 100% entry-exit system. These criticisms fail to recognize the necessity of deploying US–VISIT in manageable stages to ensure success. Before Secretary Ridge took the bold step of allowing an entry-exit system to be built in increments, year after year went by with no deployment because nobody could figure out how to deploy a universal system that would actually find unwanted criminals and terrorists without crippling international trade and sparking outrage among the business persons, students, and tourists we need to attract to our country. Under the incremental system, we now have biometric review of all foreign visitors except diplomats, children, and the elderly at our air and sea ports, all visa holders at our busiest land ports of entry, and certain visitors departing the country at designated air and sea ports.

In addition to US–VISIT, DHS has utilized biometrics to facilitate secure travel across our northern and southern borders with the NEXUS and SENTRI programs. An even more ambitious international registered traveler program was announced by Secretary Ridge in January of this year to expedite known international travelers through immigration and customs processing.

An important and overdue integration of biometric systems occurred over the past year when CBP reached full integration of its Border Patrol facilities utilizing the IDENT fingerprint booking system with the FBI's IAFIS fingerprint system. This capability, reached ahead of schedule, means that CBP will be aware of any undocumented immigrants detained by the Border Patrol whose fingerprints reside in the IAFIS system because they have a prior criminal conviction or outstanding warrant, or left a latent fingerprint at a crime scene. CBP can thus make more informed decisions as to whether to detain such an individual or allow him or her to accept voluntary departure due to overcrowding in ICE detention space.

While these programs are aimed at foreign visitors, biometrics will soon play a key role in the security of passports issued to American citizens. Under the electronic passport program being developed by the Department of State and the Government Printing Office, U.S. passports will include a biometric facial image and biographic information which will be read via a contactless chip by passport readers deployed by DHS. The United States, like many countries around the world developing biometric passports, has seen deployment of this round of e-passports delayed while technical issues have been ironed out in international organizations and privacy concerns have been addressed. It is clear, however, that a well-designed U.S. passport program is essential to securing our own borders to detect foreign imposters and perhaps even those entitled to a U.S. passport with ties to terrorism or serious criminal behavior. It is more important to deploy an effective program utilizing the best technology and procedures available than to rush pilot portions of the program out the door. I have great faith in the Department of State team to navigate these difficult issues and produce this necessary result.

Also, while not the subject of this hearing, TSA has been building our biometrically-based systems to support the Registered Traveler program, to conduct background checks of HAZMAT drivers and foreign flight crews, and to secure access to

sterile areas of transportation facilities through the Airport Access Control program and the Transportation Worker Identification Card. And, of course, numerous agencies have been improving their use of biometrically enhanced identification documents for employees and contractors, a process that will improve significantly with the full implementation of Homeland Security Presidential Directive 12 issued by the President in August of 2004.

US–VISIT

For many years after it was technologically possible, the United States lacked an automated entry and exit system that would allow us to know when foreign visitors arrive and when they depart. Following the bombing of the first World Trade Center in 1993, Congress demanded that an entry and exit system be installed at our ports of entry, but it did not happen, and none was in place on 9/11. Remarkably, on that date INS continued to rely on a paper system, and employees literally hand-keyed in departure information into a database weeks after the fact. With no exit system, and only a minimal, unreliable entry system, our entry and exit data was spotty at best, and criminals were able to come and go across our border, some of them dozens of times under different aliases, without detection.

But in 2004, DHS rolled out the entry-exit system known as "US–VISIT". We improved on the Congressional plan by adding a biometric requirement to the system. To capture biometrics, US–VISIT electronically scans a visitor's index fingers and takes a digital photograph at a kiosk—all in the space of seconds. The biometrics captured by US–VISIT allow consular and immigration officials to confidently tie travelers to the visas and passports they are carrying, and permit the development of an internationally uniform standard for identifying travelers.

As of May 31, 2005, DHS has enrolled 28,169,895 travelers in US–VISIT, with each watchlist check taking an average of 6 seconds. US–VISIT has allowed DHS to unravel the assumed identities of hundreds of foreign nationals attempting to unlawfully enter the United States. For example, an individual sought admission after flying into Newark International Airport. Everything appeared normal until his fingerprints were scanned. It turns out that the man was traveling under an alias and was in fact a convicted rapist. He had previously been deported from the United States, and had a traveled here before, using 9 different aliases and 4 dates of birth. US–VISIT has helped us to identify and to reject over 600 other undesirable individuals. These cases have utilized information originally collected in many different settings: by DOS during visa applications into the Consolidated Consular Database; by FBI during crime investigations into the IAFIS database; by foreign governments into Interpol; and by intelligence services. It is not possible to know how many terrorists or criminals have been frightened away from attempting to enter our country because of US–VISIT, but I have no doubt that the number is substantial.

However, certain analyses of the program, most notably a major piece in May 23's *Washington Post*, have misunderstood the program and the decisions that led to its staged deployment.

The article insinuates that key decisions made concerning US–VISIT were made by a handful of program officials and government contractors. Nothing could be further from the truth. Nearly all aspects of the program have undergone exacting scrutiny from the White House Office of Management and Budget and the Homeland Security Council, following robust debate and interaction with other key departments including Justice, State, and Commerce. During my tenure at DHS, Secretary Tom Ridge, Under Secretary Asa Hutchinson, Customs and Border Protection Commissioner Robert Bonner, and many others were intimately involved in developing policy guidance, interacting with other federal agencies and foreign governments, and supervising operations. The US–VISIT program team, led by Director Jim Williams, deserves great credit for effectively managing the program but they have done so under tight direction from the DHS leadership.

The 9/11 Commission took a hard look at the US–VISIT and basically said that DHS was on the right track, just to deploy the system more quickly. As the program tackles difficult increments ahead, the public should know that its public servants have, despite immense technological and political challenges, deployed a system that truly has enhanced our security without destroying the attractiveness of the United States as a place to study, conduct research or business, or see friends or family. In short, US–VISIT is a government program that actually works.

VISA WAIVER PROGRAM

As it is the most recent development in this area, the announcement last week by DHS Secretary Chertoff concerning the application of the statute requiring biometric identifiers established by the International Civil Aviation Organization for travelers utilizing passports issued after October 26, 2005 for travel to the U.S. under the Visa Waiver Program merits discussion. I believe the outcome announced

by DHS is an appropriate one. The original, and worthy, goal of the Enhanced Border Security and Visa Entry Reform Act of 2002 was to leverage the international nature of ICAO to bring biometrics to the border. The decision by ICAO to mandate a digital facial image which could be compared to the person presenting the passport could represent a marginal increase in security by detecting persons with forged or stolen passports. However, the software that will allow such effective comparisons in actual field environments without generating unacceptable numbers of false positives is still under development. Allowing an additional year until October of 2006 to ensure interoperability of documents and document readers and enhancements to the facial recognition software is a wise decision. In addition, the damage to our economic relations and to the willingness of VWP countries and the European Union to work cooperatively on border management issues that enforcement of this year's deadline would have caused hardly would have been worth the marginal improvements in security possible this year. It is also very important to remember that when the EBSVERA was enacted, there was no US–VISIT program to find terrorists or criminals about whom we have biometric information. Thus a reinterpretation of a somewhat vague statute to reflect changed circumstances is a reasonable resolution of a looming crisis.

NEXT STEPS FOR USING BIOMETRICS TO SECURE OUR BORDERS

However, while the programs described above represent effective use of biometrics, this technology can and should provide significantly greater benefits to securing our borders and facilitating legitimate travel. Among the key recommendations I would like to provide the Committee to best put biometric technology to work include:

- Transition to 10-Fingerprint Collection

It appears to have been somewhat forgotten amid the success of the 2-fingerprint system utilized by US–VISIT, but DHS promised from the beginning that a transition to 8 or 10 prints would be necessary at some point to address two separate weaknesses with the 2-print program. First, leading scientists at NIST and elsewhere have long believed that an IDENT database populated by millions of 2-print records would eventually begin to generate unacceptable levels of false matches. While I am not aware that this scenario has begun to occur, it must be tackled ahead of a crisis. Second, I understand that a small but potentially important number of latent fingerprints collected from crime scenes or terrorist investigations may elude matching in IDENT if they come from different digits, such as from thumbs, than are collected under US–VISIT. Deploying 10-print readers to consular posts abroad and U.S. ports of entry is a necessary transition over the next several years.

While many have discussed this issue in the context of the relative merits of the IDENT and the FBI's IAFIS fingerprint databases, the need for DHS and DOS to capture 10 fingerprints should not lead one to conclude that our border management systems could be based on the IAFIS system. IAFIS was not designed to run on a real-time basis, meaning it is an unlikely candidate to serve as the platform for an entry-exit system. DHS requested fingerprints held in IAFIS to load into IDENT and has received increasing cooperation from DOJ in this regard, but it is critical to remember that the overwhelming majority of IAFIS prints are of U.S. citizens who do not register with US–VISIT. The linkages between the systems need continued improvement but it would take a major overhaul of IAFIS to even consider utilizing it for real-time entry-exit purposes.

- Collection of Fingerprints in U.S. Passports

The United States has never advocated mandatory collection of fingerprint information in foreign passports, in part because it has never required that U.S. citizens provide fingerprints in their own passport applications. This decision needs to be reexamined. In part due to this decision, the United States and the larger world community are building out two elaborate but conflicting border management systems. In the first, governments are going to great lengths to collect terrorist fingerprints along with biographic information, to share such information with other governments, and to ensure that agencies within their government are sharing relevant fingerprints. Within the U.S. government alone, massive efforts have been expended to ensure sharing of relevant biometric information between agencies. In the second system, countries are building elaborate systems of tamper-resistant passports and passport readers capable of doing biometric comparisons; however, neither the mandatory biometric of facial recognition nor one of the optional biometrics, iris scan, can be utilized to find a known terrorist or criminal from a database, because such databases do not exist.

The historical resistance of governments to fingerprint law-abiding citizens, not only in the U.S. but in Japan, Australia, and numerous other nations, is weakening.

The collective weight of the 28 million enrollments in US–VISIT is huge. The program applies to all nationalities and races, has generated no privacy complaints, and has not impacted the speed of border crossings. At a time when terrorists have killed large numbers of people in Asia, Europe, Africa, and other areas of the globe, in addition to North America, people are understandably willing to put aside nervousness about fingerprinting in order to cut off the lifeblood of terrorists—mobility across borders.

Thus I recommend that the U.S. match the bold step of the European Union to include fingerprints in passports and that the U.S. should advocate for fingerprints as a mandatory biometric in passports at ICAO. At a time when we are going to great lengths to build anti-terrorism and law enforcement systems based on fingerprints, we will never be able to fully engage other countries if we decline ourselves to do what is needed. Taking this step for U.S. citizens who travel internationally might also allow us to avoid a national identification card that many believe is appropriate for border security purposes.

Of course the U.S. government could attempt to build a regime to allow one-to-one biometric check between the person who applied for a passport and the person appearing for reentry to the U.S. based on an iris, hand geometry or facial recognition match. Such a system, however, leaves extensive fingerprint information unutilized and denies us the "bully pulpit" to ask ICAO and other governments to march down the fingerprint path. It is also worth noting that current policy does not allow U.S. applicants to be vetted biometrically against criminal or terrorist databases before they are issued passports, meaning we may miss potential imposters or homegrown terrorists or criminals. Nor are we in a strong position to ask other countries to vet their applicants against watchlists they maintain or have rights to access. I am encouraged by the strong efforts of DOS to vet applicants against name-based databases such as the Terrorist Screening Center and certain lists of persons with outstanding warrants, but a fingerprint capability would augment those efforts considerably.

- Biometrics Are The Solution at Our Land Ports of Entry

The next handful of years will see a convergence of major initiatives affecting how traffic flows across our land borders with Mexico and Canada: the deployment of US–VISIT to primary lanes of our land ports of entry and exit; the requirement that U.S. citizens, Canadians, and residents of certain Caribbean nations present a secure travel document to enter or reenter the U.S.; and the possibility of a new guest worker program to ensure that foreign workers able to pass a security check are allowed to work for willing employers in the U.S. These three issues need to be considered in conjunction as border management systems are developed.

First, it is absolutely critical that the Congress aggressively fund US–VISIT so that land border implementation is not delayed. This project is extremely difficult but essential. Travel documents for Mexican nationals, most significantly Border Crossing Cards used for millions of trips a year, must be retrofitted or reissued to include information capable of being read wirelessly at land ports of entry. Entry traffic lanes must be constructed or altered to allow for wireless connectivity to identify watchlist or criminal hits in time for an inspector to refer a potential entrant to secondary processing. While it may not be feasible to conduct a one-to-one check on all applicants (i.e., is the person holding the identification card the same person to whom it was issued), a one-to-many check (i.e. does the information on the card indicate a watchlist hit) should be feasible.

The exit feature of the land borders is no less daunting as we currently have no exit infrastructure at all. A reasonable goal over the next several years is construction of a system that will inform DHS whether persons departing the U.S. have complied with the terms of their entry, with relationships built with Mexican and Canadian authorities to assist with the very rare case of a departing individual who needs to be apprehended immediately.

In addition, I understand that maintaining current levels of funding for US–VISIT may delay full implementation of the exit component at air and sea ports. DHS has had enough pilot testing done on a variety of biometric exit models involving kiosks, departure receipts, and gate confirmation to make decisions on the best system to deploy. It is time to round out that aspect of our entry-exit system to identify those who violate the terms of their visa and the occasional but important instances where a known terrorist or violent criminal is attempting to depart the country. US–VISIT's recent identification of a sexual predator seeking to leave the country in Texas is a great example of an exit enforcement capability. I also believe that having a robust exit system may allow the country to consider changes to the current statutory standard that visa applicants prove that they are unlikely to overstay their visas.

Lastly, US–VISIT's end state will include a "person-centric" inventory of all relevant enforcement and immigration services information. When fully-funded and implemented, the program should put an end to the unwieldy and confusing system of records maintained regarding travel and immigration and will result into better service to legitimate travelers and students, and better enforcement tools as well.

Second, the passage of the Western Hemisphere Travel Initiative last year as part of the intelligence bill means that millions of U.S. citizens returning the U.S. and many Canadians and nationals of certain Caribbean nations will be required to produce a secure travel document such as a passport or SENTRI or NEXUS card beginning in 2008. I congratulate the Congress for this important security enhancement, but recognize that the law will create immense workload challenges for DOS and lifestyle changes for border residents. This increased workload makes the challenges to deploy US–VISIT and next generation passports all the more important.

Third, discussion about a temporary worker program has intensified since President Bush's 2004 request that Congress enact such a program in line with his immigration principles. Some commentators have presented the issue as a choice between a new worker program and enhanced border security. Such analysis is wrong. It is the passage of a properly developed guest worker program that will bring massive improvements in border security and thus homeland security. Millions of undocumented aliens have crossed the border illegally in search of work who present no risk of terrorism or organized criminal activity. Border Patrol agents in the field, however, have no way to differentiate between the individuals that make up this flood of human migration and the small but crucial number of potential terrorists or criminals that attempt to blend into the masses. Providing those who want to work and have no prior criminal or terrorist record a means to enter the country legally through ports of entry will make it much more likely that the Border Patrol will be able to locate and arrest the criminals and terrorists who will lose their cloak of invisibility that the current situation offers.

However, those who are skeptical of this argument have understandable reasons for this view. For decades, enforcement tools to combat illegal immigration went underutilized, underfunded, or unsupported by the employer community. While DHS has made substantial progress in enforcing the current regime, deploying a new guest worker program will require significant new resources for border and employer enforcement and for port of entry operations and facilities, development and issuance of tamper-proof identification documents, streamlining of the legal regimes that adjudicate the status of border crossers and undocumented aliens, and new avenues of cooperation between the U.S. and Mexican government.

All of these enhancements to our current enforcement posture should support a basic motto of any new legislation: "deter and reward." Those who are seeking to enter our country to work must be faced with a reality that crossing our borders illegally or attempting to work without proper certifications will be detected and punished with long-term consequences for violations. In contrast, those that follow the rules on applying for work, passing a security check, and crossing the border legally should be able to work and receive retirement and travel privileges.

Among the specific recommendations I would like to provide the Committee concerning the proposed temporary worker program related to biometrics are the following:

- Interview and Criminal History Background Checks: Any new applicant should be required to submit ten fingerprints for a IDENT and IAFIS review to demonstrate, in addition to any employment criteria designed to ensure that the entrant's employment is not likely to be filled by a U.S. worker, that he or she has no ties to terrorism or history of prior criminal behavior other than non-violent illegal entry to the U.S.;
- Use of Biometrically-Enhanced Identification Documents: Any new entrant should be required to obtain a unique, biometrically-enhanced identification document that can serve as a document for entry under US–VISIT at a port of entry and as an employment verification document;
- Employment "Insta-check": Employers should only be able to hire new temporary workers from outside the U.S. after DHS and fellow agencies have developed and deployed a "insta-check" system pulling biometric information off travel documents to verify eligibility for employment and reviewing Social Security and driver's license numbers from new workers asserting U.S. citizenship;

These proposals address the machinery by which new entrants, legal and illegal, should be handled. Of course, any new temporary worker program also must be structured to allow existing undocumented workers to apply for employment. The security imperative for this class of aliens is that they undergo a vetting for ties to terrorism and criminal behavior before they are authorized for further employ-

ment in the U.S. Understanding that a principal reason for the program is to continue an adequate supply of workers for current jobs, there is no reason that this security review cannot be conducted while the worker remains in the U.S. However, just as one of our bedrock principals of our overseas visa process is collection of biometrics by a trained U.S. government official to ensure that the applicant is not an imposter, consideration should be given to requiring provision of biometrics by this population to a U.S. government official, especially if the resulting document will be utilized for international travel.

- International Registered Traveler Programs

A key component of continuing to attract foreign travelers to the U.S. should be an international registered traveler program. This program would build on the existing CBP NEXUS and SENTRI programs for land and air travel between the U.S., Canada, and Mexico and bring to life the vision of Secretary Ridge's January 2005 announcement of such a pilot operating between the Netherlands and the U.S. While it would be beneficial to travelers who undergo enhanced vetting to receive preferential treatment at a foreign departure airport, the main use of biometrics would be to exempt IRT enrollees from normal immigration and customs processing at U.S. ports of entry. Enrollees would simply have their travel documents scanned at a kiosk, provide fingerprints to ensure a match to the documents, and proceed to pick up their luggage. This system will require construction of real-time connectivity to the IRT kiosks. On the front end, enrollees would need to be vetted for any connection to inadmissible behavior, including terrorism, criminal behavior or prior immigration violations. Especially for Visa Waiver Program travelers who have not been required to undergo a terrorism check because they did not apply for a visa, such a scrub will need to be thorough and include an interview by a trained U.S. inspector. If done correctly, the program would be an excellent example of risk management to enable CBP to focus on riskier visitors. It would also send a strong signal to the customers, clients, and coworkers of the world, whose travel we need to be able to expedite, that the U.S. is open for business.

- International Cooperation

By definition, border management systems involve international cooperation, and the effectiveness of our use of biometrics will depend greatly on our ability to operate effectively in the bilateral and multilateral environments. Negotiating information-sharing agreements or playing a leading role in international standards-setting bodies may not be as sexy as deploying new high-tech biometric equipment but both are crucial to our success.

Developing information-sharing agreements with foreign partners is a laborious process that has to deal with varying privacy regimes, technical challenges, and concerns about revealing sources and methods of intelligence. However, we know that terrorists and other criminals must use international travel to develop their plots and the development of robust sharing agreements of biometric and biographic watchlist information should be a high priority. Especially with allies like the United Kingdom and Canada, these types of agreements dramatically increases the odds of using travel checkpoints to find those who need to be detected.

I would make a special mention of the European Union's Visa Information System due to come on-line in the next several years. Having negotiated the treaty on airline passenger data with the EU last year, I know how difficult it may be to build interoperability between the VIS and our BioVisa/US–VISIT program. Now is the time to begin to tackle that challenge as our citizenries should expect these systems to share valuable intelligence when they are both operational.

In addition, DHS needs to increase dramatically its engagement with foreign governments and international standards setting bodies such as ICAO. The proposed merging of the BTS Policy office, the DHS Office of International Affairs, and other policy entities in DHS into a robust policy office is a necessary first step. DHS needs to develop a cadre of country specialists and DHS attaches to represent the department in key international locations and to ensure that DHS policymaking does not stop at the water's edge.

CONCLUSION

I congratulate the Committee and Subcommittee for its continued cooperation with and oversight of DHS and its component agencies. I thank you for the opportunity to appear before you today and look forward to your questions.

Mr. LUNGREN. Thank you very much, Mr. Verdery, for your testimony.

The Chair will now recognize Mr. Gregory Wilshusen, the director of information security issues for the Government Accountability Office.

And at the end of the testimony of our entire panel, I would suggest we go over and vote and then come back. We will have about a half-hour period before the next vote.

STATEMENT OF GREGORY WILSHUSEN, DIRECTOR OF INFORMATION SECURITY ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. WILSHUSEN. Thank you, Mr. Chairman, Ranking Member Sanchez and members of the subcommittee. I am pleased to be here today to present a summary of GAO's work on radio frequency identification, or RFID, technology. As requested, I will present a brief overview of RFID technology and discuss the security, privacy and other considerations associated with its implementation. My testimony today is based upon GAO's recently issued report on this topic.

RFID is an automated data capture technology that can be used to electronically identify, track and store information contained on electronic chip or tag. A radio frequency reader scans the tag for stored information and transmits the information to a database or display device using wireless communications.

Several federal agencies have already begun testing and using this technology, including the State Department, which plans to use it in its electronic passport. The proposed U.S. electronic passport is to have an embedded contactless chip. The chip is to store the same information printed on the data page of the passport and will include a digital photograph.

Several security issues are associated with federal and commercial use of RFID technology. These issues relate to protecting the confidentiality, integrity and availability of the information on the tags and in the databases.

In particular, key security considerations include ensuring that only authorized readers or personnel can access or read the information on the tags and in the databases, maintaining the integrity of that information, ensuring that critical data is fully available when needed and protecting against attacks such as skimming, which is the surreptitious reading of electronic information without the holder's knowledge, and eavesdropping, the interception of information from the tag while it is being read by another reader.

Without effective security controls, data on the tag can be read by any compliant reader, data transmitted through the air can be intercepted and read by unauthorized devices, and data stored in the databases can be accessed by unauthorized users.

Information security tools and practices are available to address these issues. Complying with a risk-based framework mandated by the Federal Information Security Management Act of 2002, or FISMA, and employing encryption and authentication technologies can help agencies achieve a stronger security posture.

Among the key privacy issues are using the technology to obtain or process information about an individual without that individual's knowledge or consent, tracking an individual's movements and profiling an individual's habits, tastes or predilections.

The Privacy Act of 1974 limits federal agencies' use and disclosure of personal information, and the privacy impact assessments required by the E–Government Act of 2002 provide a framework for agencies to follow in assessing the impact on privacy when implementing RFID technology.

Additional controls are proposed to mitigate privacy issues, such as using as the deactivation mechanism on the tag and incorporating blocking technology to disrupt transmission are in progress.

In addition to security and privacy, there are other issues to consider when implementing this technology. These include the interoperability and reliability of the tags and readers, the placement and orientation of the tags and the cost and benefits associated with implementation.

To summarize, the use of RFID technology can provide many benefits; however, security, privacy and other considerations need to be adequately addressed in any implementation of this technology.

Mr. Chairman, this concludes my statement. I look forward to your questions.

[The statement of Mr. Wilshusen follows:]

United States Government Accountability Office

GAO

Testimony

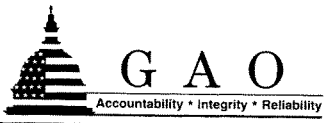
Before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, House Committee on Homeland Security

For Release on Delivery
Expected at 11:00 A.M. EDT
June 22, 2005

INFORMATION SECURITY

Key Considerations Related to Federal Implementation of Radio Frequency Identification Technology

Statement of Gregory C. Wilshusen, Director
Information Security Issues



GAO-05-849T

GAO
Accountability · Integrity · Reliability

Highlights

Highlights of GAO-05-849T, a testimony to the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, House Committee on Homeland Security

Why GAO Did This Study

Radio frequency identification (RFID) is an automated data-capture technology that can be used to electronically identify, track, and store information contained on a tag that is attached to or embedded in an object, such as a product, case, or pallet. Federal agencies have begun implementation of RFID technology, which can offer them new capabilities and efficiencies in operations. For example, the State Department has reported plans to use RFID technology in its electronic passports. The development of inexpensive tags has created a revolution in RFID adoption and has made the wide-scale use of them a real possibility for government and industry organizations.

As requested, this testimony will provide an overview of the technology and discuss key security, privacy, and other considerations surrounding implementation of the technology in the federal government. It is based on our recently issued report (GAO-05-551).

www.gao.gov/cgi-bin/getrpt?GAO-05-849T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Greg Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

June 2005

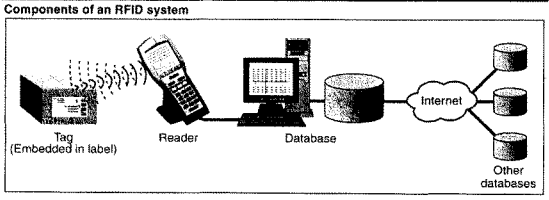
INFORMATION SECURITY

Key Considerations Related to Federal Implementation of Radio Frequency Identification Technology

What GAO Found

The main technology components of an RFID system are a tag, reader, and database. A reader scans the tag for data and sends the information to a database, which stores the data contained on the tag (see figure).

Components of an RFID system



Source: GAO.

The use of tags and databases raises important security considerations related to the confidentiality, integrity, and availability of the data on the tags, in the databases, and in how this information is being protected. Tools and practices such as implementing the risk-based framework mandated by the Federal Information Security Management Act of 2002 and employing encryption and authentication technologies can help mitigate these security considerations.

Key privacy concerns include notifying individuals of the existence or use of the technology; tracking an individual's movements; profiling an individual's habits, tastes, or predilections; and allowing for secondary uses of the information. Tools and practices can help mitigate these considerations, including existing requirements contained in legislation and proposed measures such as a deactivation mechanism on the tag, among others.

In addition to security and privacy, there are other areas of consideration related to the adoption of the technology. These areas include the reliability of the tags and readers; placement and orientation of the tag; costs and benefits associated with implementation; availability of tags; and environmental issues, such as the reuse and recycling of tags.

Abbreviations

CFO	Chief Financial Officer
DOD	Department of Defense
EPA	Environmental Protection Agency
FCC	Federal Communications Commission
FISMA	Federal Information Security Management Act
RFID	radio frequency identification
UHF	ultrahigh frequency

GAO
Accountability * Integrity * Reliability

June 22, 2005

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to present a summary of our work in the area of radio frequency identification (RFID) technology.[1] RFID is an automated data-capture technology that can be used to electronically identify, track, and store information contained on a tag. The tag can be attached to or embedded in the object to be identified, such as a product, case, or pallet. RFID provides identification and tracking capabilities by using wireless communication to transmit data.

The technology can provide a more efficient method for federal agencies, manufacturers, retailers, and suppliers to collect, manage, disseminate, store, and analyze information on inventory, business processes, and security controls, among other functions, by providing real-time access to information. Several federal agencies have already begun testing and using the technology. For example, the State Department has reported plans to use RFID technology in its electronic passports.

As requested, in my testimony today, I will present an overview of RFID technology and discuss the security, privacy, and other considerations surrounding RFID technology implementation in the federal government.

My testimony today is based on our recently published report[2] on RFID technology and was prepared in accordance with generally accepted government auditing standards.

[1]GAO, *Information Security: Radio Frequency Identification Technology in the Federal Government*, GAO-05-551 (Washington, D.C.: May 27, 2005.)

[2] GAO-05-551.

Results in Brief

RFID is an automated data-capture technology that can be used to electronically identify, track, and store information contained on a tag. The main technology components of an RFID system are a tag, reader, and database. A radio frequency reader scans the tag for data and sends the information to a database, which stores the data contained on the tag. Passive tags do not contain their own power source, such as a battery. The development of these inexpensive tags has created a revolution in RFID adoption and made wide-scale use of them a real possibility for government.

Several security and privacy issues are associated with federal and commercial use of RFID technology. The security of tags and databases raises important considerations related to the confidentiality, integrity, and availability of the data on the tags, in the databases, and in how this information is being protected. Tools and practices to address these security issues, such as compliance with the risk-based framework mandated by the Federal Information Security Management Act (FISMA) of 2002[3] and employing encryption and authentication technologies, can help agencies achieve a stronger security posture. Among the key privacy issues are notifying individuals of the existence or use of the technology; tracking an individual's movements; profiling an individual's habits, tastes, or predilections; and allowing secondary uses of information. The Privacy Act of 1974 limits federal agencies' use and disclosure of personal information,[4] and the privacy impact assessments required by the E-Government Act of 2002 provide an existing framework for agencies to follow in assessing the impact on privacy when implementing RFID technology.[5] Additional measures proposed to mitigate privacy issues, such as using a deactivation mechanism on the tag, incorporating blocking technology to disrupt

[3]44 U.S.C. § 3544 (b).

[4]5 U.S.C. § 552 a(a)(4).

[5]44 U.S.C. § 3501 note. See Office of Management and Budget M-03-22, Sept. 26, 2003.

transmission, and implementing an opt-in/opt-out framework for consumers are in progress.

In addition to security and privacy, there are other areas to consider related to the adoption of the technology. These areas include the reliability of the tags and readers, which do not consistently work with some products or in certain situations; placement and orientation of the tag, which can contribute to how effectively a tag can be read; costs and benefits associated with implementation; availability of tags; and environmental issues related to the reuse and recycling of tags.

Background

RFID technology uses wireless communication in radio frequency bands to transmit data from tags to readers. A tag can be attached to or embedded in an object to be identified, such as a product, case, or pallet. A reader scans the tag for data and sends the information to a database, which stores the data contained on the tag. For example, tags can be placed on car windshields so that toll systems can quickly identify and collect toll payments on roadways.

Interest in RFID technology began during World War II and has increased in the past few years. During the war, radio waves were used to determine whether approaching planes belonged to allies or enemies. Since then, exploration in radio technology research and development in commercial activities continued through the 1960s and evolved into marked advancements in the 1970s by companies, academic institutions, and the U.S. government. For example, at the request of the Department of Energy, Los Alamos National Laboratory developed a system to track nuclear materials by placing a tag in a truck and readers at the gates of secure facilities. This is the system used today in automated toll payment systems.

The technology offers several improvements over its predecessor technologies, such as barcodes and magnetic stripe cards. For instance, a tag can carry more data than a barcode or magnetic stripe and can be reprogrammed with new information if necessary. Additionally, tags do not typically require a line of sight to be read,

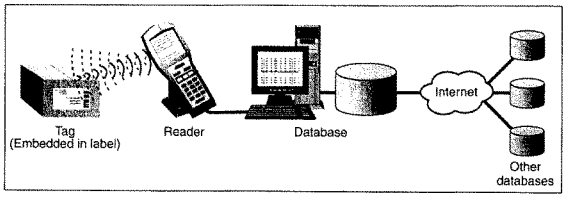
as barcodes do, and can be read more rapidly and over greater distances. Mandates by large retailers and the Department of Defense (DOD) requiring their top suppliers to use RFID tags, along with technological advancements and decreased costs, have spurred the proliferation of this technology. RFID technology is now being used in a variety of public and private-sector settings, ranging from tracking books in libraries to authenticating a key in order to start a vehicle.

RFID Technology Overview

RFID is an automated data-capture technology that can be used to electronically identify, track, and store information contained on a tag. A radio frequency reader scans the tag for data and sends the information to a database, which stores the data contained on the tag.

The main technology components of an RFID system are the tag, reader, and database. (See fig. 1.)

Figure 1. Main Components of an RFID System



Source: GAO.

The Tag

An RFID tag, or transponder, consists of a chip and an antenna. A chip can store a unique serial number or other information based on the tag's type of memory, which can be read-only, read-write, or write-once read-many. The antenna, which is attached to the microchip, transmits information from the chip to the reader.

Typically, a larger antenna indicates a longer read range. The tag is attached to or embedded in an object to be identified, such as a product, case, or pallet, and can be scanned by mobile or stationary readers using radio waves.

The simplest version of a tag is a **passive tag**. Passive tags do not contain their own power source, such as a battery, nor can they initiate communication with a reader. Instead, the tag responds to the reader's radio frequency[6] emissions and derives its power from the energy waves transmitted by the reader. Under perfect conditions, the tags can be read[7] from a range of about 10 to 20 feet.[8] The cost of passive tags ranges from 20 cents to several dollars. Costs vary based on the radio frequency used, amount of memory, design of the antenna, and packaging around the transponder, among other tag requirements. Passive tags can operate at various frequencies. Examples of passive tag applications include mass transit passes, building access badges, and consumer products in the supply chain. The development of these inexpensive tags has created a revolution in RFID adoption and made wide-scale use of them a real possibility for government and industry organizations.

Semipassive tags[9] also do not initiate communication with the reader but contain batteries that allow the tag to perform other functions, such as monitoring environmental conditions and powering the tag's internal electronics. These tags do not actively transmit a signal to the reader. Some semipassive tags remain dormant (which conserves battery life) until they receive a signal from the reader. The battery is also used to facilitate information storage. Semipassive tags can be connected to sensors to store information for container security devices.

[6]Frequency is the number of radio waves that pass a given point during a fixed period of time (e.g., the number of complete oscillations per second of energy).

[7]The read range of a tag is based on the size of the antenna, frequency used, power of the reader, and the material between the tag and the reader.

[8]Although these tags can theoretically be read at 30 feet, when factoring in circumstances that can interfere with the read range (e.g., water and metal), the actual read distance is reduced to 10 feet or less.

[9]Semipassive tags are also referred to as semiactive or battery-assisted passive tags.

Active tags contain a power source and a transmitter, in addition to the antenna and chip, and send a continuous signal. These tags typically have read/write capabilities—tag data can be rewritten and/or modified. Active tags can initiate communication and communicate over longer distances—up to 750 feet, depending on the battery power. The relative expense of these tags makes them an option for use only where their high cost can be justified. Active tags are more expensive than passive, costing about $20 or more per tag. Examples of active tag applications are toll passes, such as "E-Z pass," and the in-transit visibility applications on major items and consolidated cargo moved by DOD.

Tags have various types of memory, including read-only, read-write, and write-once read-many. Read-only tags have minimal storage capacity (typically less than 64 bits) and contain permanently programmed data that cannot be altered. These tags primarily contain item identification information and have been used in libraries and video rental stores. Passive tags are typically read-only. In addition to storing data, read-write tags can allow the data to be updated when necessary. Consequently, they have larger memory capacity and are more expensive than read-only tags. These tags are typically used where data may need to be altered throughout a product's life cycle, such as in manufacturing or in supply chain management. A write-once, read-many tag allows information to be stored once, but does not allow subsequent alterations to the data. This tag provides the security features of a read-only tag while adding the additional functionality of read/write tags.

The Reader

In order for an RFID system to function, it needs a reader, or scanning device, that is capable of reliably reading the tags and communicating the results to a database. A reader uses its own antenna to communicate with the tag. When a reader broadcasts radio waves, all tags designated to respond to that frequency and within range will respond. A reader also has the capability to communicate with the tag without a direct line of sight, depending on the radio frequency and the type of tag (active, passive, or semipassive) used.

Readers can process multiple items at once, allowing for increased read processing times. They can be mobile, such as handheld devices that scan objects like pallets and cases, or stationary, such as point-of-sale devices used in supermarkets. Readers are differentiated by their storage capacity, processing capability, and the frequencies they can read.

The Database

The database is a back-end logistic information system that tracks and contains information about the tagged item. Information stored in the database can include item identifier, description, manufacturer, movement of the item, and location. The type of information housed in the database will vary by application. For instance, the data stored for a toll payment system will be different than the data stored for a supply chain. Databases can also be linked into other networks, such as the local area network, which can connect the database to the Internet. This connectivity can allow for data sharing beyond the local database from which the information was originally collected.

RFID Systems Operate on Radio Frequencies

Choice of radio frequency is a key operating characteristic of RFID systems. The frequency largely determines the speed of communication and the distance from which the tag can be read. Generally, higher frequencies indicate a longer read range. Certain applications are more suitable for one type of frequency than other types, because radio waves behave differently at each of the frequencies. For instance, low-frequency waves can penetrate walls better than higher frequencies, but higher frequencies have faster data rates. RFID systems use an unlicensed frequency range, classified as industrial-scientific-medical or short-range devices, which is authorized by the Federal Communications Commission (FCC).[10] Devices operating in this unlicensed bandwidth may not

[10]In the United States, the FCC authorizes the use of the 2.4 GHz and the 902-928 MHz frequency range for industrial-scientific-medical and short-range devices, which includes RFID technology.

cause harmful interference and must accept any interference received. The FCC also regulates the specific power limit associated with each frequency. The combination of frequency and allowable power levels determine the functional range of a particular application, such as the power output of readers.

The U.S. Department of State has reported plans to use RFID technology in its electronic passports.[11] The United States and other countries are anticipating using the International Civil Aviation Organization[12] (ICAO) Document 9303 standard, which prescribes an international format for passports, visas, and other official machine-readable travel documents.

Security and Privacy Considerations with RFID

The security of tags and databases raises important considerations concerning the confidentiality, integrity, and availability of the data on the tags, in the databases, and in how this information is being protected. Measures to address these security issues, such as compliance with the risk-based framework mandated by the Federal Information Security Management Act (FISMA) of 2002 and employing encryption and authentication technologies, can help achieve a stronger security posture. Among the key privacy issues are notifying individuals of the existence or use of the technology; tracking an individual's movements; profiling an individual's habits, tastes or predilections; and allowing for secondary uses of information. Measures to mitigate these issues are in progress.

[11]The proposed U.S. electronic passport will resemble a regular passport with the addition of a small RFID chip embedded in the back cover. The chip will securely store the same data visually displayed on the photo page of the passport and will also include a digital photograph.

[12]ICAO was chartered by the United Nations to regulate international aviation and includes the United States and 188 other nations.

Security Considerations Relate to Data Confidentiality, Integrity, and Availability

Several agencies identified data confidentiality, integrity, and availability as key security considerations with implementing RFID technology. Specifically, these issues included ensuring that only authorized readers or personnel have access to information, maintaining the integrity of the data on the chip and stored in the databases, and ensuring that critical data is fully available when necessary. Other issues with implementing the technology included the potential for various attacks, such as counterfeiting or cloning,[13] replay,[14] and eavesdropping; the possibility of electronic collisions when multiple tags and/or readers are present; and the presence of unauthorized components that may interfere or imitate legitimate system components.

Without effective security controls, data on the tag can be read by any compliant reader; data transmitted through the air can be intercepted and read by unauthorized devices; and data stored in the databases can be accessed by unauthorized users.

Practices and Tools in Place to Address Security Considerations

Using security practices and tools such as the risk-based framework mandated by FISMA, encryption, and authentication can help mitigate the security considerations associated with implementing RFID technology.

Implementing the security practices required in FISMA can help strengthen the security of RFID systems that store information transmitted from tags. FISMA requires each agency, including agencies with national security systems, to develop, document, and implement an agencywide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those

[13]Cloning an RFID tag occurs when an attacker produces an unauthorized copy of a legitimate tag.

[14]A replay attack is an attack in which a valid data transmission is maliciously or fraudulently repeated, either by the originator or by an adversary who intercepts the data and retransmits it.

provided or managed by another agency, contractor, or other source. Specifically, this program is to include

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;
- risk-based policies and procedures that cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout the life cycle of each information system;
- subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems;
- security awareness training for agency personnel, including contractors and other users of information systems that support the operations and assets of the agency;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, performed with a frequency depending on risk but no less than annually, and which includes testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems;
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;
- procedures for detecting, reporting, and responding to security incidents; and
- plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

Encrypting the data on the tags, in the air, or stored in a database may also reduce the risk of unauthorized use or changes. Using encryption may be particularly relevant for applications where sensitive information is contained on the tag. Encryption is the process of transforming ordinary data (commonly referred to as plaintext) into code form (ciphertext) using a special value known as a key and a mathematical process called an algorithm. Cryptographic algorithms are designed to produce ciphertext that is unintelligible to unauthorized users. Decryption of ciphertext is

possible by using the proper key. Encryption technologies can be used to (1) hide information content, (2) prevent undetected modification, and (3) prevent unauthorized use. When properly implemented, encryption technologies may provide assurance regarding the confidentiality, integrity, or origin of information that has been exchanged. It may also provide a method by which the authenticity can be confirmed. Without strong encryption, the data may not be kept confidential.

Authentication, which is the process of verifying the claimed identity of a user, can be used between tag and reader as a way to mitigate security risks. Authentication of readers can help prevent the unauthorized reading and/or writing to tags.

Privacy Issues Surrounding RFID Use

The extent and nature of the privacy issues related to the federal and commercial use depends on the specific proposed use. For example, using the technology for generic inventory control would not likely generate substantial privacy concerns. However, the use of RFIDs by the federal government to track the movement of individuals traveling within the United States could generate concern by the affected parties. Privacy issues associated with RFID implementation include notifying individuals of the existence or use of the technology; tracking an individual's movements; profiling an individual's habits, tastes or predilections; and allowing for secondary uses of information.

- **Notification.** Individuals may not be aware that the technology is being used unless they are informed that the devices are in use. Therefore, unless they are notified, consumers may not be aware that the RFID tags are attached to or embedded in items they are browsing or purchasing or that the items purchased are being scanned.

- **Tracking.** Tracking is real-time, or near-real-time, surveillance in which a person's movements are followed through RFID scanning. Media reports have described concerns about ways in which anonymity is likely to be undermined by surveillance. As previously reported, many civil liberties groups are concerned about the

application of this technology to track individuals' movements, such as in a public school setting, and the resulting loss of anonymity in public places.[15] Additionally, periodic public surveys have revealed a distinct unease with the potential ability of the federal government to monitor individuals' movements and transactions.

- **Profiling.** Profiling is the reconstruction of a person's movements or transactions over a specific period of time, usually to ascertain something about the individual's habits, tastes, or predilections. Because tags can contain unique identifiers, once a tagged item is associated with a particular individual, personally identifiable information can be obtained and then aggregated to develop a profile of the individual. As previously reported,[16] profiling for race, ethnicity, or national origin has caused public debate in recent years. Both tracking and profiling can compromise an individual's privacy and anonymity.

- **Secondary uses.** In addition to issues about the planned uses of such information, there is also concern surrounding the possibility that organizations could develop secondary uses for the information; that is, information collected for one purpose tends over time to be used for other purposes as well. This has been referred to as "mission-" or "function-creep." The history of the Social Security number, for example, gives ample evidence of how an identifier developed for one specific use has become a mainstay of identification for many other purposes, governmental and nongovernmental.[17] Secondary uses of the Social Security number have been a matter not of technical controls but rather of changing policy and administrative priorities.

The widespread adoption of the technology can contribute to the increased occurrence of these privacy issues. As previously

[15]GAO, *Technology Assessment: Using Biometrics for Border Security*, GAO-03-174 (Washington, D.C.: Nov. 15, 2002).

[16]GAO-03-174.

[17]GAO, *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards*, GAO-02-352 (Washington, D.C.: May 31, 2002).

mentioned, tags can be read by any compatible reader. If readers and tags become ubiquitous, tagged items carried by an individual can be scanned unbeknownst to that individual. Further, the increased presence of readers can provide more opportunities for data to be collected and aggregated. As the uses of technology proliferate, consumers have raised concerns about whether certain collected data might reveal personal information such as medical predispositions or personal health histories and that the use of this information could result in denial of insurance coverage or employment to the individual. For example, the use of RFID technology to track over-the-counter or prescription medicines has generated substantial controversy.

Practices and Tools to Mitigate Privacy Issues Are in Progress

Implementing privacy practices and tools, such as existing requirements contained in the Privacy Act of 1974 and the E-Government Act of 2002, and employing proposed measures such as a deactivation mechanism on the tag, blocking technology to disrupt transmission, and an opt-in/opt-out framework for consumers can help mitigate some of these privacy issues. These proposed techniques may address some of the privacy issues and are in progress.

An existing legal framework that addresses the privacy issues under which federal agencies operate when implementing any new information technology is defined in the Privacy Act of 1974, which limits federal agencies' use and disclosure of personal information. The act's protections are keyed to the retrieval of personal information by a "name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph."[18] The Privacy Act generally covers federal agency use of personal information, regardless of the technology used to gather it. As a practical matter, however, the Privacy Act is likely to have a limited application to the implementation of RFID technology because the act only applies to the information once it is collected, not to whether or how to collect

[18]5 U.S.C. §552a(a)(4).

it. The E-Government Act's privacy impact assessments requirement, however, provides a means of evaluating whether or not to collect information based on privacy concerns.

Employing a mechanism that can deactivate, or "kill," a tag at the point of sale, can prevent tracking of the individual and item once the tag leaves a store. This feature would still provide the supply chain tracking benefits to the retailer without providing additional information about the consumer beyond the point of sale. However, enforcement may be a challenge, as a tag may inadvertently be deactivated or remain dormant with the potential to be reactivated. Additionally, consumers opting to have the tags deactivated may have to undergo additional procedures that may cost time or money.

Another proposed method is blocking technology. Devices that can disrupt the transmission of all or selected information contained on a tag would be embedded in an object that is carried or worn near RFID tags that the individual wants blocked. This technology, however, has not yet been fully developed. One challenge to its development may be the constant proximity required between the blocker tag and the tag in order to disrupt data transmission. Consumers may not consistently remember to juxtapose the tags, thereby reducing the effectiveness of the technology. A physical method of blocking currently in use is aluminum-coated Mylar[19] bags, which can absorb or diffuse RFID signals when placed over the tag. An example is in toll payment systems where aluminum-coated Mylar bags are issued along with the tag so that drivers can place their tags in the bag to prevent them from being read inadvertently. Additionally, the State Department is reported to have plans to include metal inside U.S. passport jackets to help prevent the chip from being read by anyone except customs and border agents.

Government and industry groups have also proposed using an opt-in/opt-out framework. This framework would provide consumers with an option to voluntarily participate in RFID transactions that

[19]Mylar is a registered trademark of Dupont Tejin Films that generally refers to plastic film. A common application is packaging film for food, electronics, and medical devices.

gather data about them. Consumers would be informed of the existence of the tags and the type of information that would be collected and could then decide whether to participate in the transaction or opt out. A concern of this hybrid system is the potential disparity in benefits received between consumers who opt in versus those who opt out, similar to customer loyalty cards, and the notion that this framework might penalize consumers who articulate their privacy preferences. Also, a study by the RAND Corporation has suggested that organizations using RFID workplace access devices should implement "fair information practices" and communicate those policies to employees.[20]

Other Areas of Consideration Are Relevant to RFID Adoption

In addition to privacy and security, other areas of consideration related to the adoption of RFID technology include the reliability of tags and readers, the placement of the tags, the costs and benefits of implementation, the availability of tags, and environmental issues.

Reliability. Currently, tags are not always reliable and will not work with some products or in certain situations. When something close to the reader or tag interferes with the radio waves, read-rate accuracy decreases. For instance, defective tags created by the manufacturer can be unreadable or tags may be damaged during the supply chain process. Additionally, readers can produce false negatives (a reader does not read a valid tag that passes within the prescribed range) or false positives (a tag not intended to be read inadvertently passes within range of a reader), which typically occur with closely packed items where multiple tags are near each other. Further, environmental conditions, such as temperature and humidity, can make tags unreadable. Experts have indicated that tags read at high speeds have a significant decrease in read rate. As the technology continues to mature, these limitations may eventually be addressed, but currently they remain a challenge to organizations.

[20]The RAND Corporation, *Privacy in the Workplace: Case Studies on the Use of Radio Frequency Identification in Access Cards*, RB-9107-RC (Santa Monica, Calif.: 2005).

Placement. The placement and orientation of the tag contributes to how effectively the reader can scan it. Factors to consider in tag placement are read and nonread points on objects such as items, cases, or pallets; locations that minimize the risk of damage to the tag and have the highest potential for a successful passive tag reading; and read points in specific environments, such as an item running through a conveyor belt at various speeds.

Some organizations, such as DOD, have documented procedures for tag placement to help ensure placement precision, consistency, and efficiency. Determining optimal tag placement may require software or an automated application to improve this otherwise manual process.

Costs and Benefits. Best practices for information technology investment dictate that prior to making any significant project investment the costs and benefits of the system should be analyzed and assessed in detail.[21] The cost of the tags generally falls on the supplier, as it is the supplier who tags the items. Retailers see benefits from RFID tags such as improved product visibility during the supply chain process. Suppliers can also see such benefits when they go beyond the "slap and ship"[22] model and find new ways to make the technology add value to gain a return on investment. According to the National Institute of Standards and Technology, smaller suppliers may earn little to no return because the costs associated with implementing the technology, such as hardware, software, infrastructure, middleware,[23] and training will be a substantial portion of a small supplier's budget. Additionally, their price per-tag may be high since they do not order large quantities. Organizations need to determine if the cost of implementing this technology, which is still in the early stages of adoption, is worth the increased ability to collect and analyze data.

[21] GAO, *Aviation Security: Challenges in Using Biometric Technologies*, GAO-04-785T (Washington, D.C.: May 19, 2004).

[22]"Slap and ship" is when a supplier tags the products with an RFID tag right before shipping them to the retailer. Suppliers who slap and ship generally will not benefit from the technology because they do not make use of it for their own benefit.

[23]Middleware is software that connects two otherwise separate applications.

Availability. With increasing adoption of RFID technology, the availability of tags may emerge as a growing concern. The increased adoption of the technology will result in greater demand for tags. As a result, the demand for tags may eventually outstrip the supply. Even if industry can keep up with the demand, damage to the tags during production may create a shortage. For instance, according to a research group's survey of RFID vendors, up to 30 percent of chips are damaged during production when they are attached to their antennae, and an additional 10 to 15 percent are damaged during the printing process. Improving tag manufacturing and quality control processes may help increase the availability of operative tags.

Environment. In September 2004, the Environmental Protection Agency (EPA) and the Office of the Federal Environmental Executive (OFEE) cohosted a workshop on the impact of tags on the reuse and recycling of packaging materials. Tags contain silicon, adhesives, and nickel, and the antennae are typically made from copper, aluminum, or, if printed, silver. According to OFEE, these elements of the tags are potential contaminants for recyclers and manufacturers using recycled materials. As such, OFEE and EPA believe that it is essential that these industries begin to understand the potential impacts of having tags on packaging materials and pallets and plan how to minimize the impact on the environment. One manufacturer remarked on the lack of practicality in recycling because of the small amount of silicon used in the chip. Currently, EPA does not provide clear national guidelines on electronic waste (e-waste) disposal nor has it defined its e-waste goals and measures. Consequently, states are pursuing their own mechanisms to regulate e-waste. As tagging begins to include cases, additional environmental issues may arise because cases are not reusable, in contrast to the pallets, which are reusable.

In summary, RFID technology can provide new capabilities as well as an efficient method for federal agencies, manufacturers, retailers, and other organizations to collect, manage, disseminate, store, and analyze information on inventory, business processes, and security controls by providing real-time access to information. The use of the technology, however, raises several security and privacy considerations that may affect federal agencies' decisions to

implement the technology. Key security issues include protecting the confidentiality, integrity, and availability of the data and information system. The privacy issues include notifying consumers; tracking an individual's movements; profiling an individual's habits, tastes, and predilections; and allowing for secondary uses of information. In addition, other areas such as the reliability, placement, and availability of tags, along with the cost and benefits of implementation and environmental concerns, are factors to consider.

Mr. Chairman, this concludes my statement. I look forward to your questions.

Contacts and Acknowledgements

Should you have any questions about this testimony, please contact Greg Wilshusen at (202) 512-6244 or by e-mail at wilshuseng@gao.gov. Other individuals who made key contributions to this testimony include Nancy Glover, Min Hyun, Stephanie Lee, and Suzanne Lightman.

(310561)

Mr. LUNGREN. I thank the panel for their statements.

We are going to recess now to go over and vote. I am coming back. I hope some other members can come back. It is one vote. Well, it is one vote, then a 10-minute debate, then 15-minute vote—oh, they changed it now.

Well, if the gentlemen would like to start, I will let him start then.

Mr. DICKS. Let me ask you, Mr. Herman and Mr. Verdery, one of the things I was concerned about was when the decision was made by DHS to use in the US–VISIT Program 2 fingerprints versus 10 fingerprints. Now, NIST did a big study on this, and one of the concerns they had was that here you have got the FBI system that is built on 10 fingerprints and it would be much better if we had a consistent system.

And everybody on Capitol Hill was trying to tell this to the administration. We had Asa Hutchinson up here for a private meeting to explain to him that the technology with 10 is much better, and the only answer we got back was, "Well, we have to do this incrementally." This is Mr. Verdery's position. But if it is wrong and it is less effective and it is going to have to be redone, why do it? Why didn't we do it right the first time?

Dr. Herman, do you have any wisdom on this?

Mr. HERMAN. Well, this is certainly what we recommended in that 2003 report.

Mr. DICKS. Mr. Verdery, why did the administration against all of this advice go the opposite direction, which could be extremely costly if we have to redo this system?

Mr. VERDERY. A couple of things. One, it is not costly. The amount of money that went out for the readers is a pittance compared to the overall cost of the program. To deploy the little small fingerprint readers is a drop in the bucket compared to the budget of this program, much less the rest of the Department.

Second, we would have no program if we had waited to do a 10-print deployment because it would require retrofitting overseas of all the consular posts at the little windows. There is no way to put a 10-print reader there without retrofitting those offices. And also the connectivity required to build out 10-print.

Now, the things is I think people will get confused sometimes. The 10 prints has nothing to do with the fact the FBI has a 10-print system. It is more data that reduces the chance of making a mistake. But it is not because the FBI has 10, it is because you have more data.

Mr. DICKS. Yes, but you get that database, right. If you had 10 fingerprints, you would get—

Mr. VERDERY. You cannot, because IAFIS cannot work on a real-time basis. It can only work when they give us prints ahead of time and we load them into IDENT. And that is what they have been giving DHS is prints that are built into IDENT. There is no real-time connectivity at IAFIS because it does not work that way. It takes days to get an answer from IAFIS.

Mr. DICKS. Mr. Herman, do you have any comments on this?

Mr. HERMAN. Well, just that if IAFIS were to be used for background checks, there is certainly the real-time issue, I agree, but if it were to be used for background checks, it would have to be 10

fingers because IAFIS will not accept two fingers. The only way to use the FBI criminal database for background checks is to use 10 fingers.

Mr. DICKS. So by going with two fingerprints, we, in essence, eliminated the ability to use IAFIS.

Mr. VERDERY. No, no, because we requested and got cooperation slowly from the FBI to build in the prints of foreign-born criminals and people with outstanding warrants and a number of other classes into IDENT so you get that capability. It does not check on a real-time basis against all 43 million IAFIS prints, most of which are U.S. citizens because that is just not possible. If we were trying to run it as a real-time system against IAFIS, people who landed at Dulles—

Mr. DICKS. All these experts who said it was possible, all kinds of companies said it could be done, that this was a major mistake.

Mr. VERDERY. I have never seen—sorry.

Mr. DICKS. Well, we have got SAGEM Morpho, a French company who has done a number of countries, said this could have been done, 10 fingers was the right way to go, and this was a major mistake that would wind up costing a lot of money to fix later.

Now, maybe you are wrong on this but this was certainly called to the Department's attention, and to me I am still—I am glad to hear all these different views. I am still trying to find out just exactly why the Department did what it did.

Mr. VERDERY. There are separate questions. There is the 2 versus 10, which I agree, we should move to 10, but we would still be waiting to do 10 now. We would have had no system the last 2 years, this town over 600 people. We would be just doing nothing.

So that is the question, do you want the 2-print system that has a great record or nothing while you are building out the 10-print system is the first question? And the second question is, can IAFIS work as a backbone of a 10-print system, and the answer I have never seen anyone say anything but no. But I agree with you, we do need to go over 10 prints over time, as it is feasibly possible. Otherwise, you have nothing.

And just in terms of how this happened, under the law, the Attorney General, the DHS Secretary and the Secretary of State all had to agree on the two-print system and that was agreed to by Attorney General Ashcroft—

Mr. DICKS. They did not go a very good job of explaining back up here on the Hill why they felt—the effort was pretty minimal in terms of trying to explain it to us about all these facts. I am glad you explained it better.

[Recess.]

Mr. LUNGREN. I will just reconvene the subcommittee.

I am sorry, we have had some unexpected votes that are of a procedural matter, and we do not know how long that is going to go on, so rather than have you just sit here, I thought I would come back and at least get one round of questions in before I have to go back for the next vote.

Dr. Herman, according to studies by the NIST and others, various biometrics show promise in identification capabilities, the iris biometrics versus the fingerprint one; however, as far as I know, there is no existing repository of data on irises. So what is the util-

ity of that for which we are investing in those kinds of technologies?

Mr. HERMAN. Well, iris could be used for the on-to-one match. So you mentioned some programs, Registered Traveler. It can be used where checking against the terrorist database is one thing, checking to see whether you are the same person issued a travel document is different. And iris can certainly be used in that. Those are the kinds of applications that most people are think gin about for iris.

Mr. LUNGREN. Mr. Verdery, what do you say about the application of iris? Because in the back of my mind on all of this is how practical are these things, how do we make them work effectively and efficiently? It just seems to me fingerprints seem to be the most capable of being utilized for various different identification and matching purposes.

Mr. VERDERY. Well, a couple things. And you always have to think of what is the point of what you are trying to do, and, usually, this means trying to conduct a one-to-one match, as was just mentioned. Is the person standing in front of you the person that they claim they are? And also a one-to-many match is the person standing in front of you, no matter who they claim to be, are they a problem based on the terrorist database or other database? And in some cases, you are not quite as worried about the second one, access to a facility where you have got other layers of security, where you might not be as worried about a one-to-many check every time. So an iris could work in those circumstances.

But also as a good backup there are a small but when you load up the numbers a decent amount of people whose fingerprints cannot be read due to historical factors and the like, and so having a backup is very good in those kinds of cases. That is why it was done during the Registered Traveler pilot as a backup in some cases.

So, no, it is not good for finding a terrorist out of the group, but it can be used in certain specialized situations.

Mr. LUNGREN. Do you have any sense or have you seen any surveys or was there any research done on whether there is some cultural reluctance for American citizens to submit to fingerprint as opposed to iris identification?

Mr. VERDERY. I am not aware of any scientific research. I am sure there is some, but I am not privy to it. Again, I felt a little bad for my colleague, Ms. Dezenski, sitting here answering these questions when, in all actuality, the decision to go to ICAO and advocate for facial recognition as a biometric standard in documents was not DHS, it was the rest of the government. It actually occurred just before DHS came into existence in early 2003, and the State Department carried that message, but it was a U.S. government decision. It was not DHS' decision.

The question is now should we go back and try to reverse that position, and I think, again, as I testified, I think it would be a wise move, although I would not want to lead anyone into thinking that it would be met with easy success.

Mr. LUNGREN. Mr. Wilshusen, what are the privacy concerns considering RFID technology? And what has been done to improve the security of these chips?

Mr. WILSHUSEN. Well, there are several privacy issues, and these include using the technology to obtain or process information from an individual without that individual's knowledge or consent. That could be, for example, done by skimming. Also, just—

Mr. LUNGREN. How do you do that? I mean, practically, if I have got a card myself, what would—

Mr. WILSHUSEN. Well, one would need for an individual, or unauthorized user, if you will, would need to have a reader pick up the radio frequency emitted by that particular chip or tag and be able to access the data on that tag.

Mr. LUNGREN. Is that difficult technologically?

WILSHUSEN; No, not necessarily, no. It would be the same type of readers and available that are used for legitimate purposes, but it would have to be compliant and meet the same standards that are set up for that application.

Mr. LUNGREN. Do you have to be in close proximity, physical proximity?

Mr. WILSHUSEN. Generally, so, yes. How close is a matter or function of what type of chip and what radiorequency is being used in that application.

Mr. LUNGREN. So, obviously, it is whatever information is there. The information is merely the name. Okay. So name, address, birth date, which could just be as easily printed on there and someone could read it themselves.

Mr. WILSHUSEN. That is correct.

Mr. LUNGREN. What is the durability of these devices? Do we have to be concerned about how readily they can be interfered with or destroyed or through accidental exposure to water or something that renders them inoperable?

Mr. WILSHUSEN. In terms on the e-passports?

Mr. LUNGREN. Yes.

Mr. WILSHUSEN. Well, our particular review was at a government-wide level where we looked at and identified initiatives across the different agencies. We did not do an in-depth review of e-passports specifically but how long the chips can last, depends upon, their use. I will actually defer to the gentleman from NIST on how long they may last. I think there might have been a question earlier.

Mr. HERMAN. That is outside of my area of expertise. There is a different part of NIST, and I guess it needs to be explained. We do the work in the biometrics area. There is a different part of NIST that does work on RFID chips. And we could certainly get information for you if you want, but that is just outside my area of expertise.

Mr. LUNGREN. My thought is that we ought to know that. I mean, I do not know. I do not have any idea. I would hope that whatever we move to is going to last as long as the passports we have or if there is a need for us to update—I am trying to think whether there would be a need for us to update information on a regular basis, probably not.

This is just basic information, Mr. Verdery; is that correct?

Mr. VERDERY. That is right. That is right. And also, I mean, it is worth pointing out that even outside the government's fears, as important as it is, the topic of today's hearing, the commercial sec-

tor is exploding with uses of RFID, your EZ Pass and your Smart Tag at the gas station and a zillion other uses. So they are going to lead the way in the technology standards and durability for purposes outside the government perspective, and it is a huge industry, domestic suppliers, foreign suppliers, and that is going to lead the agenda here on durability and other factors.

Mr. LUNGREN. Can you tell me why it takes so long for us to develop these things? I mean, if in fact you are talking about how the private sector takes the lead on this and we have these technology changes and so forth, they seem to come with such rapidity, is it because of the privacy concerns that we have that it takes us such a long time to really kind of put these things in train and start them moving?

Mr. VERDERY. Well, I think there are a lot of different factors. I mean, when Congress passed the law in late 2002 asking for ICAO to come up with the standard, they began the motions to do that. ICAO is your typical international organization. It moves as quickly as it can but it is bringing, whatever, 187 countries into general consensus with difficult technical standards. They were moving as quickly as they can. I think the program, if Frank Moss was still here, has now been held up for some period of time due to the privacy concerns outside of kind of the ICAO process.

Mr. LUNGREN. Were you involved in the ICAO process before?

Mr. VERDERY. Tangentially. The US–VISIT staff that was within our directorate led our efforts kind of on the technical level in Montreal and other places to try to build up that technical level.

Mr. LUNGREN. Do you have any insight into why the E.U. has reluctance to share their fingerprints with us?

Mr. VERDERY. Well, I think it is a very fair question. My guess is if they were here, they would say, "Well, what are you going to share with us?" We have nothing to share with them, we do not take fingerprints. And so they have taken the step of—

Mr. LUNGREN. But we have—

Mr. VERDERY. Not in passports.

Mr. LUNGREN. Not in passports.

Mr. VERDERY. So they are building out fingerprints in their internal documents for the E.U. purposes.

Mr. LUNGREN. Right.

Mr. VERDERY. And they have said that they are currently planning on keeping that E.U.-only system a closed system. But that is all the more reason for us to be bold in doing it ourselves so we have something to negotiate with. Right now it would be a one-way trade.

Mr. LUNGREN. The suggestion I thought I got from the previous panel was that we were not doing it because the European countries would not share with us but we do not have anything, as you suggest, to share with them.

Mr. VERDERY. We can share US–VISIT.

Mr. LUNGREN. Right, I understand that, but in terms of our passport.

Mr. VERDERY. That is right. If you travel overseas, there is nothing for them to access in our passport fingerprint-wise because it is not there.

Mr. LUNGREN. Well, let me just ask you this then: What security benefits would you see coming out of us putting fingerprints on our passports beyond the US–VISIT Program?

Mr. VERDERY. Well, the benefits for us doing it on our own are a couple. One, if we ran checks of people at the time of application, you might be able to find imposters or other criminals or terrorists at the time of application and State is doing a lot now on the biographic side, as Frank testified to, but that does not catch the biometric hits that would come up.

Second, we could run those people through US–VISIT when they travel back and forth. That currently is not done. So that would again find those types of imposters or criminals if we wanted to do that.

And, third, is I think the point I was getting at before, it would allow us to offer other countries who are worried about Americans, legitimately or not, coming into their shores, allow us to build out an international system of interoperability built on travel documents.

Mr. LUNGREN. The compatibility of the fingerprint system with most of these countries around the world is not repeated with any other mechanism of identification. I mean, we have our fingerprint system for our criminal justice programs, they have their fingerprint system. I mean, fingerprint system started in England, for goodness sake.

Mr. VERDERY. You have INTERPOL as a kind of repository of that trade. But, again, that is of criminals, not of just your average tourist who has not shown up on a terrorist database.

LUNGREN; We have another vote going on there. I think I am finished with all my questions, but if you can stick around a little bit longer, I have got to find out whether my Ranking Member is coming back. Do we know? Maybe we can check. Otherwise, I might be able to let you go.

Mr. VERDERY. Sir, if I could, while we have open mike day.

Mr. LUNGREN. Open mike, right here, open mike Friday, but it is on Wednesday.

Mr. VERDERY. It does not happen very often, but I am not sure I actually responded to your question about kind of the cultural issues.

Mr. LUNGREN. Yes.

Mr. VERDERY. Again, I think the experience of world travelers coming to US–VISIT, travelers or all nations, all races, all everything, except for kids and old people and diplomats, basically having no problem with the system, takes 6 seconds. Some people think it is actually kind of cool, it is kind of neat. I think it is producing a sea change around the world as to, "Hey, look, this is no big deal."

And the other thing is that fingerprints can differentiate people who otherwise might get caught up in some kind of biographic confusion. John Smith, the terrorist, causing all the other John Smiths traveling some travel problems. The biometrics would clear that person, essentially.

And, so, again, I think there is a sea change underway. We have been leading that, I think we need to continue to lead that. But this is the first worldwide use of biometrics, and I think it has been

a great experience and hopefully has convinced travelers and governments around the world that that is the way to go.

Mr. LUNGREN. And who are excepted from that? You say children and—

Mr. VERDERY. Under 14, I think over 79 or maybe it is 69 and diplomats.

Mr. LUNGREN. And the reason for the first two being exempted from that?

Mr. VERDERY. Initially, it was a workload issue. We did not want to overload the system, and the odds of these folks being terrorists, I think, were considered to be low or visa overstayers. And so I think that was the reason. And diplomats obviously for reciprocity concerns.

Mr. LUNGREN. That is what I keep telling TSA about secondary checks of my 2-year-old granddaughter. I do not think there is much chance of her being a terrorist.

I want to thank the witnesses for appearing. I understand no one else is coming back. And I would just say for the record that some members may want to submit some written questions to you, and if they do, if you could respond in a timely fashion.

I thank you for your testimony.

And this subcommittee hearing stands adjourned.

[Whereupon, at 2:06 p.m., the subcommittee was adjourned.]

○